Risikoidentifikation und Risikosteuerung in IT-Sourcing-Netzwerken

Dissertation

der Wirtschaftswissenschaftlichen Fakultät

der Universität Augsburg

zur Erlangung des Grades eines Doktors

der Wirtschaftswissenschaften

(Dr. rer. pol.)

vorgelegt

von

Christian König

(Diplom-Kaufmann)

Augsburg, Oktober 2014

Erstgutachter:	Prof. Dr. Hans Ulrich Buhl
Zweitgutachter:	Prof. Dr. Michael Krapp
Vorsitzender der mündlichen Prüfung:	Prof. Dr. Marco C. Meier
Datum der mündlichen Prüfung:	25.11.2014

Inhaltsverzeichnis

Anmerkung: Eine fortlaufende Seitennummerierung wird pro Kapitel vorgenommen. Ein Literaturverzeichnis sowie die Anhänge werden jeweils am Ende eines Beitrags aufgeführt.

Verzeichnis der Beiträge

In dieser Dissertation werden die folgenden veröffentlichten und zur Veröffentlichung angenommenen Beiträge vorgestellt:

B1 König C (2014) Gestaltungsspielräume bei Cloud Computing Investitionen. HMD - Praxis der Wirtschaftsinformatik 51(4):494-505

VHB JOURQUAL 2.1: 5,16 Punkte, Kategorie D

B2 Buhl HU, Fridgen G, König C (2013) Using Financial Derivatives to Hedge Against Market Risks in IT Outsourcing Projects – a Quantitative Decision Model. Journal of Decision Systems 22(4):249-264

VHB JOURQUAL 2.1: 7,17 Punkte, Kategorie B

B3 Keller R, König C (2014) A Reference Model to Support Risk Identification in Cloud Networks. Accepted for: 35th International Conference on Information Systems (ICIS), Auckland, New Zealand

VHB JOURQUAL 2.1: 8,48 Punkte, Kategorie A

B4 Fridgen G, König C, Mette P, Rathgeber A (2013) Die Absicherung von Rohstoffrisiken - Eine Disziplinen übergreifende Herausforderung für Unternehmen. ZfbF Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 65(2):167-190

VHB JOURQUAL 2.1: 7,21 Punkte, Kategorie B

I Einleitung

Unternehmen nutzen das Konzept des IT-Outsourcings bereits seit mehr als 30 Jahren, um sich die notwendige Flexibilität zur Anpassung an sich verändernde Umweltbedingungen schaffen zu können (Lee et al. 2003). Des Weiteren werden mit IT-Outsourcing Ziele wie Kostensenkung, einfacher Zugriff auf zusätzliche IT-Ressourcen und die Fokussierung auf die eigenen Kernkompetenzen verfolgt (Lacity et al. 2009). In den letzten Jahren ist Cloud Computing als neues IT-Outsourcing-Paradigma entstanden (Bresnahan et al. 2011). Cloud Computing lässt sich dabei als konsequente und logische „Weiterentwicklung des etablierten Organisationskonzeptes Outsourcing auf Basis eines neuen technologischen Konzepts“ (Böhm et al. 2009) begreifen. Damit kann es im Kontext des IT-Outsourcings als neue Bereitstellungsform für IT-Leistungen betrachtet werden, die nun einfach „aus der Wolke“ bezogen werden können. Die zunehmende Bedeutung von Cloud Computing ist durch seine Kerneigenschaften, wie hoch elastische Skalierbarkeit von IT-Ressourcen, automatisierte Provisionierung zwischen Anbieter und Nutzer, sowie verbrauchsgerechte Abrechnung ohne nennenswerte Anschaffungskosten, bedingt (Mell und Grance 2011, Armbrust et al. 2009). IT-Ressourcen aus der Cloud werden für gewöhnlich in die Servicemodelle Software as a Service, Platform as a Service und Infrastructure as a Service unterteilt und können mittels der verschiedenen Liefermodelle Private Cloud, Public Cloud oder Hybrid Cloud bereitgestellt werden (Mell und Grance 2011). Cloud Computing bietet sich als eine IT-Sourcing-Lösung an, die Unternehmen dabei unterstützt, die Anforderungen an Flexibilität und gleichzeitige Kosteneinsparungen zu erreichen. Ben-Yehuda et al. (2014) gehen sogar davon aus, dass Nutzer in der Zukunft automatisierte Software-Agenten einsetzen werden, die unter ökonomischen Gesichtspunkten dynamisch IT-Ressourcen kaufen und verkaufen. Cloud Computing wirkt hier als Katalysator, welcher einen schnellen Austausch von IT-Ressourcen ermöglicht und damit das IT-Sourcing vereinfacht.

Mit der zunehmenden Adaption von Cloud Computing in der Praxis betreten viele neue Anbieter von Cloud-Lösungen den Markt. Zudem haben sich einige bereits etablierte IT-Unternehmen zu „Big Playern“ der Cloud-Industrie aufgeschwungen, wie beispielsweise Amazon, Google oder Microsoft. In diesem Marktumfeld sind verschiedene Entwicklungen festzustellen. Einerseits kann eine zunehmende Standardisierung von Cloud-Computing-Leistungen beobachtet werden (Vaquero et al. 2009), insbesondere im Bereich der Infrastrukturdienste. Standardisierung und Austauschbarkeit von Cloud-Diensten ermöglichen dabei Multisourcing-Konzepte, wie beispielsweise von König et al. (2013) untersucht. In

diesem Markt entstehen neue Geschäftsmodelle, die das Auffinden und den Austausch solch standardisierter IT-Ressourcen erleichtern und eine börsenähnliche Funktion übernehmen, analog zu den von Buyya et al. (2008) beschriebenen Cloud-Brokern. Hier sind die Deutsche Börse Cloud Exchange, die Massachusetts-Open-Cloud-Initiative oder auch die HP Aggregation Platform als Beispiele zu nennen. Des Weiteren kommt es zu einer zunehmenden Spezialisierung von Cloud-Diensten, insbesondere im Bereich des Software as a Service, wodurch die Vielfalt der angebotenen Dienste erweitert wird und auch Anforderungen spezieller Benutzergruppen bedient werden können (Höfer und Karagiannis 2010). Nutzer sind nun in der Lage, auch sehr spezielle Funktionen durch IT-Sourcing beziehen zu können (Troshani et al. 2011). Damit wird die Möglichkeit verbessert, sich auf die eigenen Kernkompetenzen zu fokussieren.

Erhöhte Austauschbarkeit von Anbietern, ein großes Angebot an Cloud-Services, sowie der einfache und teilweise automatisierte Zugriff erhöhen die Vernetzungen zwischen den Akteuren im Cloud-Computing-Markt. Des Weiteren beschränken sich die Akteure in diesem Markt oftmals nicht nur auf die Nutzung von Cloud-Services zum „Eigengebrauch“, sondern bieten auf diesen Services basierende Leistungen wieder am Markt an. So können beispielsweise Infrastrukturdienste verwendet werden, um darauf aufbauend eigene spezialisierte Applikationen zu entwickeln und diese wiederum verfügbar zu machen. Somit bestehen IT-Sourcing-Beziehungen über mehrere Akteure hinweg und es kommt zur Entstehung von komplexen IT-Sourcing-Netzwerken. Cloud Computing stellt dabei, wie zuvor bereits angemerkt, eine Form des Sourcings von IT-Dienstleistungen in diesen vernetzten Strukturen dar. Ojala und Tyrväinen (2011) und Leimeister et al. (2010) sprechen von „value networks in cloud computing“, in denen ein Nutzer IT-Leistungen von einem Anbieter bezieht, welcher das dahinter liegende Netzwerk koordiniert. Pelzl et al. (2013) nutzen den Begriff des Wertschöpfungsnetzwerks von Cloud-Anbietern. Diese Dissertation verwendet den Begriff des IT-Sourcing-Netzwerks dabei im Kontext des Sourcings von IT-Services und deren Umsetzung in Form von Cloud-Services, welche den vorgestellten Charakteristika der IT-Sourcing-Netzwerke entsprechen. Dabei können jedoch Betrachtungen von und Erkenntnisse aus weiteren (IT-)Sourcing-Beziehungen, welche – wie beispielsweise in Beitrag 2 und Beitrag 4 vorgestellt – über das Sourcing von IT-Services hinausgehen können, für Schlussfolgerungen für IT-Sourcing-Netzwerke herangezogen werden.

In diesen betrachteten IT-Sourcing-Netzwerken existieren komplexe Verflechtungen zwischen den einzelnen Akteuren, wobei viele verschiedene Akteure von einigen wenigen abhängig sind.

Die Intransparenz bezüglich der Netzwerkstruktur erschwert dabei die Auseinandersetzung mit verschiedenen Risiken, welche in IT-Sourcing-Netzwerken bestehen. Bei Betrachtung der beschriebenen Charakteristika von IT-Sourcing-Netzwerken fällt auf, dass „klassische“ Risiken des IT-Outsourcings in den Hintergrund treten oder verändert in Form von IT-Service-, beziehungsweise Cloud-spezifischen Risiken auftreten. Unter Risiken des IT-Outsourcings sind beispielsweise Wechselkosten zwischen Providern, ein starker Kostenanstieg, versteckte Kosten oder schlechte Servicequalität zu subsumieren (vergleiche Aubert et al. 2002). Im Bereich der Cloud-Computing-Risiken werden in der Literatur unter anderem Risiken in Bezug auf die Verfügbarkeit des Services, Lock-In-Gefahr, Probleme bei Datensicherheit und Datenschutz oder auch der Ausfall eines Anbieters genannt (vergleiche Armbrust et al. 2010, Troshani et al. 2011, Clarke 2010, Clarke 2012, AlZain et al 2012).

Aufgrund des vernetzten Zusammenspiels der verschiedenen Akteure in IT-Sourcing-Netzwerken genügt es jedoch nicht, sich allein auf eine statische Betrachtung der Risiken in bilateralen Verhältnissen zwischen Anbietern und Nutzern zu beschränken. Über den Fluss der IT-Leistungen, die über mehrere Akteure hinweg gehandelt werden, können sich auch bestehende Risiken zwischen den verschiedenen Akteuren ausbreiten. Dabei begünstigt eine starke Vernetzung zwischen den Akteuren die dynamische Ausbreitung von Risiken im Netzwerk, wodurch weitere verbundene Akteure mit diesen Risiken infiziert werden. So führte beispielsweise ein Unwetter über Dublin im August 2011 zu Ausfällen der Cloud-Angebote von Amazon (Amazon Elastic Compute Cloud EC2) und Microsoft (Microsoft Business Productivity Online Suite BPOS), nachdem ein Stromausfall die Datencenter beider Anbieter getroffen hatte. Daraus resultierend war es für Nutzer dieser Angebote nicht mehr möglich, ihre darauf basierenden Produkte (beispielsweise auf Amazons EC2 gehostete Webangebote) weiterhin für die eigenen Kunden bereitzustellen (Miller 2011). Am vorgestellten Beispiel wird ebenfalls ersichtlich, dass bestimmte Risiken auch mehrere Akteure zugleich treffen können, was in gewissen Fällen zu einer Verstärkung der Auswirkungen für das gesamte IT-Sourcing-Netzwerk führen kann. Eine Verstärkung der Risiken erfolgt ebenfalls aufgrund der „fehlenden Unabhängigkeit der Einzelrisiken in einer Cloud-Infrastruktur“ (Haas und Hofmann 2013), zum Teil ergeben sich die Risiken dabei auch erst aus der dynamischen Komplexität des IT-Sourcing-Netzwerks selbst (vergleiche die Definition von Neitzke (2007) zu systemischen Risiken). Somit ist das Risiko für einen Akteur nicht mehr nur von den eigenen Aktivitäten und der Wahl des direkten Sourcing-Partners abhängig, sondern ebenfalls von den Abhängigkeiten zu vielen weiteren Akteuren im IT-Sourcing-Netzwerk über verschiedene Sourcing-Partner

hinweg. In solchen komplexen Systemen muss die „Genetik und Funktionsweise von Systemen mit der Eigenschaft hoher Komplexitäten der sie regierenden Interdependenzen“ (Schließmann 2010) verstanden werden, um diese Risiken geeignet adressieren zu können. Dies gilt nicht nur für die Finanzwirtschaft, sondern auch für die Realwirtschaft und das Produkt IT-Leistung.

Hierbei wird der ambivalente Charakter der Informationstechnologie in diesem Kontext ersichtlich. Einerseits ermöglicht sie für Unternehmen neue Chancen durch den einfachen Bezug und Austausch von IT-Ressourcen und die Genese neuer Applikationen zur Abdeckung verschiedenster Aufgabengebiete. Andererseits begründet sie „als Enabler einer immer globaleren, vernetzteren und schnelleren Welt“ (Buhl 2013) die angesprochene Existenz, Ausbreitung und Verstärkung von Risiken in solchen IT-Sourcing-Netzwerken, insbesondere da sie nicht nur als Treiber, sondern gleichzeitig als schnell und einfach handelbares Produkt in Form von IT-Services auftritt. Um die Wettbewerbsfähigkeit und damit das langfristige Überleben der Akteure in diesem vernetzten Markt sicherzustellen, ist die Beherrschung dieser Risiken notwendig (Junginger 2005). Ein hierzu erforderliches Risikomanagement beinhaltet im Allgemeinen die Phasen Risikoidentifikation, Risikobewertung, Auswahl und Durchführung von Maßnahmen zur Risikosteuerung sowie Evaluation und Monitoring der Ergebnisse (vergleiche Stoneburner et al. 2001, Hallikas et al. 2004).

Im Bereich des Managements von IT-Outsourcing oder Cloud-Computing-Risiken existieren verschiedene Risikomanagementansätze, bei denen der Fokus zumeist auf die bilaterale Perspektive gesetzt wird, in welcher ein Auftraggeber oder Nutzer von Cloud-Services die anbieterseitigen Risiken adressieren möchte. Tafti (2005) stellt beispielsweise ein Rahmenwerk zur Identifikation von IT-Outsourcing-Risiken vor und Willcocks et al. (1999) untersuchen verschiedene Ansätze des Risikomanagements im IT-Outsourcing und deren jeweilige Auswirkungen. Zhang et al. (2010) entwickeln ein Rahmenwerk zum Risikomanagement für Risiken im Bereich der Datensicherheit in der Cloud, welches jedoch auch für verschiedene weitere Risiken im Bereich Cloud Computing adaptierbar erscheint. Saripalli und Walters (2010) beschränken sich mit ihrem Ansatz ebenfalls auf Sicherheitsrisiken in der Cloud und liefern ein Rahmenwerk zur Bewertung dieser Risiken.

Betrachtet man nun vernetzte Strukturen, so sind auch hier dieselben Phasen des Risikomanagements relevant (Hallikas et al. 2004). Insbesondere im Bereich des Supply Chain Managements existieren aufgrund der Strukturverwandtheit bereits viele Ansätze und Rahmenwerke zum Risikomanagement. So schlagen Hallikas et al. (2002) und Hallikas et al. (2004) Rahmenwerke zur Identifikation und Bewertung von Risiken in vernetzten Strukturen

vor. Ritchie und Brindley (2007) entwickeln ein allgemeines Rahmenwerk zum Risikomanagement in Lieferantennetzwerken. Norrman und Jansson (2004) beschreiben ein Vorgehen zur Identifikation, Bewertung und Steuerung von Risiken in Lieferantennetzwerken im Kontext eines Ausfalls eines Vorproduzenten und Trkman und McCormack (2009) fokussieren sich mit ihrem Ansatz auf die Identifikation und Vorhersage von Risiken auf Basis bestimmter Attribute von Vorproduzenten und der jeweiligen Umweltbedingungen im Netzwerk.

Das Risikomanagement für die Domäne der IT-Sourcing-Netzwerke hat bisher jedoch erst wenig Aufmerksamkeit in der Literatur erfahren. Diese Dissertation adressiert die Risikoidentifikation und Untersuchung möglicher Risikosteuerungsmechanismen als Teilbereiche des Risikomanagements von IT-Sourcing-Netzwerken. Hierzu werden als Grundlage zunächst Risiken in bilateralen IT-Sourcing-Beziehungen betrachtet und Ansätze zur Identifikation und Steuerung dieser Risiken vorgestellt. Anschließend wird der Fokus auf Netzwerkstrukturen erweitert, für die ebenfalls Ansätze zur Risikoidentifikation und Risikosteuerung betrachtet werden. Ansätze zur Steuerung der Risiken sind oftmals eng mit der Identifikation dieser Risiken verknüpft, weshalb sich eine initiale Fokussierung auf diese beiden Teilaspekte des Risikomanagements in IT-Sourcing-Netzwerken anbietet. Die Erkenntnisse aus diesen Beiträgen stellen demnach eine Grundlage für einen künftigen holistischen Ansatz zum Risikomanagement in IT-Sourcing-Netzwerken dar, in dem auch die Aspekte der Risikobewertung auf Basis der Risikoidentifikation und des Monitorings adressiert werden müssen, um die Wahl und exakte Ausgestaltung der möglichen Risikosteuerungsansätze zu bestimmen und zu verbessern.

Der nachfolgende Abschnitt I.1 stellt Aufbau und Ziele der Dissertation in einer Übersicht (Abb. I-1) dar, während im darauf folgenden Abschnitt I.2 die zugehörigen Forschungsbeiträge in den Forschungskontext eingebettet sowie die inhaltlichen Zusammenhänge der Beiträge erläutert werden. Dazu werden ebenfalls in Abschnitt I.2 die spezifischen Forschungsfragen der Beiträge vorgestellt.

I.1 Zielsetzung und Aufbau dieser Dissertationsschrift

I. Einleitung	
Ziel I.1:	Darstellung der Zielsetzung und des Aufbaus der Arbeit
Ziel I.2:	Fachliche Einordnung und Motivation der zentralen Forschungsfragen
II. Risikoidentifikation und Risikosteuerung in bilateralen IT-Sourcing-Beziehungen (B1 und B2)	
Ziel II.1:	Darstellung einer Struktur zur Identifikation von Cloud-Computing-spezifischen Einflussfaktoren auf Ertrag, Risiko und Komplexität bei Cloud-Computing-Investitionsentscheidungen
Ziel II.2:	Strukturierte Darstellung bestehender Gestaltungspielräume und deren Auswirkungen auf realisierbare Potenziale und Risiken zur optimierten Gestaltung von Cloud-Computing-Investitionen
Ziel II.3:	Entwicklung einer Methode zur Risikosteuerung von Marktrisiken bei IT-Outsourcing-Projekten
Ziel II.4:	Untersuchung der Vorteilhaftigkeit der entwickelten Methode in Abhängigkeit verschiedener Einflussfaktoren
III. Risikoidentifikation und Risikosteuerung in Netzwerkstrukturen (B3 und B4)	
Ziel III.1:	Entwicklung einer Darstellungsform für vernetzten IT-Sourcing-Beziehungen zur Erhöhung der Transparenz in Netzwerkstrukturen von Cloud-Computing-Akteuren
Ziel III.2:	Identifikation und Strukturierung bestehender Risiken in Cloud-Computing-Netzwerkstrukturen und Untersuchung und Darstellung der dynamischen Ausbreitung dieser Risiken in solchen Strukturen
Ziel III.3:	Strukturierte Identifikation von Rohstoffrisiken anhand eines Rahmenwerks unter Berücksichtigung von Zuliefernetzwerken sowie verschiedenen Märkten und Regularien im Unternehmensumfeld
Ziel III.4:	Untersuchung möglicher Absicherungsmaßnahmen zur Risikosteuerung von Rohstoffrisiken im Unternehmensumfeld
IV. Ergebnisse und Ausblick	
Ziel IV.1:	Zusammenfassung der zentralen Erkenntnisse der Dissertationsschrift
Ziel IV.2:	Aufzeigen künftigen Forschungsbedarfs

Abb. I-1 Aufbau und Ziele der Dissertationsschrift

I.2 Fachliche Einordnung und fokussierte Forschungsfragen

Die in dieser Dissertation enthaltenen Beiträge B1 bis B4 adressieren die Aspekte der Risikoidentifikation und der Risikosteuerung in bilateralen IT-Sourcing-Beziehungen und in Netzwerkstrukturen. Sie lassen sich wie in Abb. I-2 dargestellt in den skizzierten Forschungsrahmen einordnen:

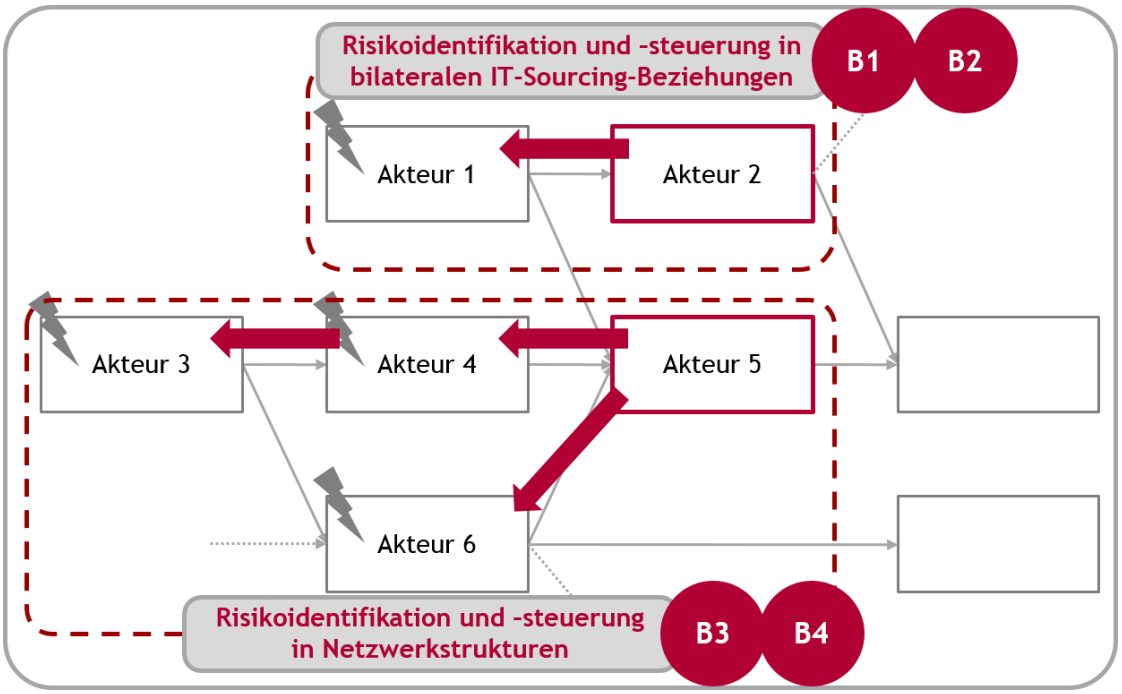

Abb. I-2 Einordnung der Beiträge der Dissertationsschrift

In der abstrahierenden Darstellung Abb. I-2 repräsentiert die Beziehung zwischen Akteur 1 und Akteur 2 die bilaterale Perspektive als Teil des Gesamtnetzwerks. Hier obliegt Akteur 2 als Nutzer die Identifikation und anschließende Steuerung von Risiken, welche durch Akteur 1 als Anbieter entstehen. Im Gegensatz dazu kann sich die Identifikation und Steuerung für Akteur 5 nicht auf die Risiken von Akteur 4 beschränken. So steht Akteur 4 in Abhängigkeit zu Akteur 3 und auch Akteur 6 als Anbieter für Akteur 5 wird selbst ebenfalls durch Akteur 3 und möglicherweise weitere Akteure beeinflusst. Hier ist also eine auf das zugrunde liegende Netzwerk erweiterte Betrachtung notwendig, die jedoch Erkenntnisse aus den bilateralen Beziehungen berücksichtigen sollte.

I.2.1 Kapitel II: Risikoidentifikation und Risikosteuerung in bilateralen IT-Sourcing-Beziehungen (Beiträge 1 und 2)

Kapitel II widmet sich zunächst bilateralen IT-Sourcing-Beziehungen als Teilaspekt von IT-Sourcing-Netzwerken. Hierbei wird der Aspekt der Risikoidentifikation und Risikosteuerung aus Sicht des Nutzers betrachtet, welcher (i) vor einer Investitionsentscheidung in Cloud-Computing-Services steht und dabei über die Ausnutzung der vorhandenen Handlungsspielräume entscheiden kann (Beitrag 1). Des Weiteren steht der Nutzer (ii) vor der Möglichkeit, ein identifiziertes Risiko im Kontext eines IT-Outsourcing-Projektes unter Ertrags-/Risikogesichtspunkten optimal abzusichern (Beitrag 2).

Cloud Computing als neue Form des IT-Sourcings ermöglicht die flexible Nutzung von IT-Ressourcen. Investitionsentscheidungen bezüglich dieser Ressourcen aus der Cloud müssen konsequenterweise im Rahmen des IT-Portfoliomanagements des Unternehmens mitgeplant werden und sollten dabei unter ökonomischen Aspekten bestmöglich ausgestaltet werden. Ziel ist eine Steigerung des Unternehmenswerts, wobei gleichzeitig die einzugehenden Risiken und Abhängigkeiten beachtet werden müssen (Zimmermann 2008). Entsprechend betrachtet Beitrag 1 diese Entscheidungssituation und trägt den vielfältigen Gestaltungsmöglichkeiten von Cloud-Computing-Investitionen Rechnung. Je nach Ausgestaltung der Investition fallen resultierende Erträge, Risiken und Abhängigkeiten unterschiedlich aus. Im Beitrag wird eine Strukturierung dieser Gestaltungsmöglichkeiten anhand von drei Dimensionen vorgeschlagen. Die Flexibilität des Liefermodells adressiert dabei den Spielraum zwischen den verschiedenen Cloud-Computing-Liefermodellen (oder Delivery Models) (vergleiche Mell und Grance 2011). So sind beim Bezug von Cloud-Services aus einer Public Cloud beispielsweise Verfügbarkeitsrisiken anders geartet als bei der Wahl eines hybriden Liefermodells. Unter der Flexibilität des Servicemodells wird die Wahlmöglichkeit zwischen unterschiedlichen Servicearten in der Cloud verstanden. Die Unterscheidung in Infrastruktur-, Plattform- und Softwaredienste (Mell und Grance 2011) spiegelt sich ebenfalls in Art und Ausmaß verschiedener resultierender Risiken wider, beispielsweise beim Risiko eines Serviceausfalls, welches aufgrund höherer Komplexität bei Softwarediensten stärker zum Tragen kommt als bei Infrastrukturdiensten. Die zeitliche Flexibilität stellt auf Handlungsoptionen ab, die während der Investitionslaufzeit zu Verfügung stehen und ebenfalls die vorhandenen Risiken beeinflussen. So kann beispielsweise durch Desinvestition und Anbieterwechsel auf ausfallgefährdete Anbieter reagiert werden. Um diese Entscheidungen ökonomisch fundiert treffen zu können, müssen die zu betrachtenden Einflussfaktoren auf Erträge, Risiken und

Abhängigkeiten identifiziert und strukturiert werden, bevor eine Steuerung der Erträge, Risiken und Abhängigkeiten durch Wahl der geeigneten Investitionsform ermöglicht wird.

Beitrag 1 adressiert dabei die folgenden Forschungsfragen:

F. 1.1 Welche Cloud-Computing-spezifischen Erträge, Risiken und Komplexitäten existieren bei Cloud-Computing-Investitionsentscheidungen? Wie können diese strukturiert dargestellt werden, um deren Identifikation zu unterstützen?

F. 1.2 Wie können die bestehenden Gestaltungsspielräume genutzt werden, um Cloud-Computing-spezifische Erträge, Risiken und Komplexitäten zu steuern?

Beitrag 2 untersucht einen konkreten Ansatz zur Steuerung eines IT-Outsourcing-Risikos. Dabei stehen Marktrisiken im Mittelpunkt der Betrachtung, die unabhängig von Durchführung des IT-Outsourcing-Projektes selbst sind. Als Beispiel ist hier der Zusammenbruch des Anbieters Baan zu nennen, was viele Kunden zum Überdenken ihrer Outsourcing-Strategie anregte (Baker et al. 2000). Das untersuchte Risiko ist dabei nicht nur in Bezug auf klassische IT-Outsourcing-Projekte von Relevanz, sondern auch im Zusammenspiel zwischen Cloud-Computing-Akteuren. Beispielsweise würde ein Ausfall von Amazon als großem Cloud-Computing-Anbieter zu massiven Problemen bei seinen Kunden führen. Erschwerend kommt im Bereich des Cloud Computing hinzu, dass in einem solchen Fall oftmals unternehmenskritische Daten verloren wären. Marktrisiken auf Seiten des Anbieters können sich in Form einer Insolvenz oder aufgrund eines starken Verlustes des Aktienkurses darstellen und in finanziellen Schäden für den Nutzer resultieren. Auch wenn solche Umstände tendenziell selten auftreten, so sind die möglichen Auswirkungen im Ernstfall als äußerst kritisch einzuschätzen. Um langfristig erfolgreich zu sein, muss ein Anbieter demnach auch solche seltenen, aber schweren Risiken betrachten. Das in Beitrag 2 vorgestellte mathematische Modell basiert auf einem Hedging-Ansatz mittels von Finanzderivaten zur Absicherung des möglichen Schadens. Dabei beschränkt sich das Vorgehen nicht auf die bisher in der einschlägigen Literatur propagierte Bewertung von IT-Projekten mittels von Finanzderivaten (vergleiche Benaroch 2002), sondern zielt auf den konkreten Kauf solcher Instrumente ab.

Beitrag 2 untersucht dabei die folgenden Forschungsfragen:

F. 1.3 Wie können Marktrisiken im Kontext von IT-Outsourcing-Projekten mittels einer Methode zur Risikosteuerung auf Basis des Einsatzes von Finanzderivaten adressiert und erfolgreich abgesichert werden?

F. 1.4 Wie wirken sich verschiedene Einflussfaktoren auf die optimale Absicherungsstrategie aus und in welchen Fällen sollte auf andere Methoden zur Risikosteuerung zurückgegriffen werden?

I.2.2 Kapitel III: Risikoidentifikation und Risikosteuerung in Netzwerkstrukturen (Beiträge 3 und 4)

Kapitel III erweitert den Fokus der Risikoidentifikation und Risikosteuerung nun von bilateralen Beziehungen hin zu Netzwerkstrukturen. Zunächst wird (i) ein IT-Sourcing-Netzwerk aus verschiedenen Cloud-Computing-Akteuren betrachtet, in dem Intransparenz bezüglich der Struktur des Netzwerks und den sich darin ausbreitenden Risiken besteht (Beitrag 3). Des Weiteren wird (ii) aufgrund der verwandten Struktur die Identifikation und Absicherung von Rohstoffrisiken untersucht (Beitrag 4). Nicht nur stellen Rohstoffe wie Metalle der seltenen Erden die Grundlage für Hightech-Produkte und damit für die Informationstechnologie selbst dar, auch lassen sich ähnliche Problemstellungen in Liefernetzwerken von Rohstoffen wie von IT-Leistungen erkennen und übertragen. Somit kann die Kenntnis von Ansätzen zur Risikoidentifikation und Risikosteuerung in Rohstoffliefernetzwerken künftig auch für die Gestaltung solcher Methoden für IT-Sourcing-Netzwerke herangezogen werden.

Die steigende Akzeptanz von Cloud Computing und die zunehmende Verbindungen zwischen einzelnen Akteuren führt, wie eingangs beschrieben, zur Entstehung von netzwerkartigen Strukturen und neuen Risiken. Diese Strukturen weisen dabei ähnliche Eigenschaften auf wie Lieferantennetzwerke (vergleiche Hallikas et al. 2002). Um diese neuen Risiken geeignet adressieren zu können, muss zunächst Transparenz in Bezug auf die zugrunde liegenden Cloud-Computing-Netzwerkstrukturen geschaffen werden und die Ausbreitung der Risiken innerhalb dieser Strukturen verstanden werden. Bestehende Forschung im Bereich von vernetzten Cloud-Computing-Akteuren, wie beispielsweise Böhm et al. (2010) oder Leimeister et al. (2010), berücksichtigt bisher nicht den Risikoaspekt. Im Hinblick auf diese Forschungslücke wird in Beitrag 3 ein Referenzmodell auf Basis der semi-formalen Modellierungssprache UML entwickelt, welches Netzwerke aus verschiedenen Cloud-Computing-Akteuren darstellt und existierende Risiken und deren Ausbreitung abbilden kann. Als Grundlage werden dabei zunächst auf Basis bestehender Literatur im Bereich Cloud Computing und anderen strukturell verwandten Disziplinen wie den angesprochenen Lieferantennetzwerken oder auch der Finanzindustrie zwei Taxonomien für verschiedene Akteure und Risiken entwickelt. Das

Referenzmodell wurde in Interviews mit Branchenexperten verbessert und wird mittels einer Instanziierung exemplarisch angewendet. Eine abschließende Diskussion zur Anwendbarkeit des Modells adressiert Aspekte wie die notwendige Informationsgewinnung und die Zuordnung der Anwendungsverantwortung im Zusammenspiel der Netzwerkakteure. Das entwickelte Referenzmodell stellt sowohl eine Basis für künftige Ansätze zur Risikobewertung dar als auch für eine Umsetzung eines Risikomanagementprozesses in Form einer IT-gestützten Lösung.

Beitrag 3 beantwortet damit die folgenden Forschungsfragen:

F. 2.1 Welche Akteure existieren in Cloud-Computing-Netzwerkstrukturen, in welchen Beziehungen stehen diese zueinander und wie können diese Strukturen dargestellt werden?

F. 2.2 Welche Risiken existieren in Cloud-Computing-Netzwerkstrukturen, wie breiten sich diese darin aus und wie kann diese dynamische Ausbreitung dargestellt werden?

Beitrag 4 beschäftigt sich mit Risikoidentifikation und Risikosteuerung von Rohstoffrisiken aufgrund der strukturverwandten Problemstellung. Auch hier befindet sich das Unternehmen in einem Netzwerk aus verschiedenen Akteuren und Einflüssen, wie seinem Kunden- und Zuliefernetzwerk, dem angeschlossenen Finanzmarkt und der Rohstoffbörse sowie Regularien aus den jeweils relevanten Rechtssystemen. Diese Akteure und Einflüsse führen einerseits zur Entstehung diverser Risiken, andererseits ermöglichen sie auch verschiedene Möglichkeiten zur Steuerung dieser Risiken, wobei Risiken in einem Bereich nicht zwangsweise mit Maßnahmen aus demselben Bereich begegnet werden muss. So kann beispielsweise dem Risiko der Preisschwankung aufgrund von Spekulation an Rohstoffbörsen mit der Maßnahme der Lagerung im Unternehmen selbst begegnet werden, um Preis und Verfügbarkeit der benötigten Rohstoffe abzusichern. Preis und Verfügbarkeit sind insbesondere bei Rohstoffen wie den Metallen der seltenen Erden als äußerst kritisch einzuschätzen, da diese global sehr unterschiedlich verteilt (die Volksrepublik China fördert beispielsweise 97% der weltweiten Produktion, vergleiche European Commission 2010), aber bei der Herstellung von Zukunftstechnologien essentiell sind. Um diese Risiken zu steuern, ist eine Identifikation der Risiken notwendig. Hierzu wird in Beitrag 4 eine strukturierte Übersicht entwickelt, in die sowohl mögliche Risiken (Risikoidentifikation), als auch mögliche Absicherungsmaßnahmen (Risikosteuerung) eingeordnet werden. Verschiedene Risiken im Bereich von Rohstoffen haben dabei auch für IT-Sourcing-Netzwerke Relevanz. So kann der Lieferantenausfall eines Rohstoffzulieferers beispielsweise den Verfügbarkeitsrisiken bei Cloud-Services zugeordnet

werden oder auch die geologischen Risiken von Rohstoffen den Risiken durch Naturkatastrophen, wie zuvor exemplarisch am Beispiel des Unwetters in Dublin dargestellt. Künftig ist demnach auch zu untersuchen, ob bestimmte Absicherungsmaßnahmen zur Risikosteuerung von Rohstoffrisiken auch entsprechend für das Produkt IT-Leistung übertragen werden können. Hedging wurde hier exemplarisch bereits in Beitrag 2 untersucht, aber auch Diversifikation und Investition in Zulieferer könnten möglicherweise adaptierbar sein.

Zusammenfassend fokussiert Beitrag 4 die folgenden Forschungsfragen:

F. 2.3 Welche Rohstoffrisiken existieren in Zuliefernetzwerken eines Unternehmens, in den verschiedenen relevanten Märkten und aufgrund von Regularien im Unternehmensumfeld?

F. 2.4 Welche Absicherungsmaßnahmen existieren zur Risikosteuerung von Rohstoffrisiken im Unternehmensumfeld?

I.2.3 Kapitel IV: Ergebnisse und Ausblick

Abschließend werden in Kapitel IV die wesentlichen Erkenntnisse der Dissertationsschrift zusammengefasst sowie Limitationen dargestellt, bevor ein Ausblick auf künftigen Forschungsbedarf gegeben wird.

I.3 Literatur

AlZain MA, Pardede E, Soh B, Thom JA (2012) Cloud computing security: from single to multi-clouds. Proceedings of 45th Hawaii International Conference on System Sciences (HICSS), Maui, USA

Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I (2009) Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, University of California:1-23

Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I (2010) A view of cloud computing. Communications of the ACM 53(4):50-58

Aubert BA, Patry M, Rivard S (2002) Managing IT Outsourcing Risk: Lessons Learned. In: Hirschheim R, Heinzl A, Dibbern J (Hrsg) Information Systems Outsourcing in the New Economy: Emergent Patterns and Future Directions. Springer, Berlin:155–176

Ben-Yehuda OA, Ben-Yehuda M, Schuster A, Tsafrir D (2014) The Rise of RaaS: The Resource-as-a-Service Cloud. Communications of the ACM 57(7)::76-84

Baker S, Spiro M, Hamm S (2000) The Fall of Baan (int'l edition). http://www.businessweek.com/2000/00_33/b3694015.htm, Abruf am 31.08.2014

Benaroch M (2002) Managing Information Technology Investment Risk: A Real Options Perspective. Journal of Management Information Systems 19(2):43-84

Böhm M, Leimeister S, Riedl C, Krcmar H (2009) Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen. Information Management & Consulting 24(2):6-14

Böhm M, Koleva G, Leimeister S, Riedl C, Krcmar H (2010) Towards a generic value network for cloud computing. In: Altmann J, Rana OF (Hrsg) Economics of Grids, Clouds, Systems, and Services. Springer, Berlin/Heidelberg:129-140

Bresnahan J, Keahey K, LaBissoniere D, Freeman T (2011) Cumulus: an open source storage cloud for science. Proceedings of the 2nd International Workshop on Scientific Cloud Computing, San Jose, USA

Buhl HU (2013) IT als Fluch und Segen. WIRTSCHAFTSINFORMATIK 55(6):371-375

Buyya R, Yeo CS, Venugopal S (2008) Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC), Dalian, China

Clarke R (2010) Computing clouds on the horizon? Benefits and risks from the user's perspective. Proceedings of the 23rd Bled eConference, Bled, Slovenia

Clarke R (2012) A Framework for the evaluation of cloudsourcing proposals. Proceedings of the 25th Bled eConference, Bled, Slovenia

European Commission (2010) Critical raw materials for the EU: Report of the ad-hoc working group on defining critical raw materials. http://ec.europa.eu/enterprise/policies/raw-materials/files/docs/report-b_en.pdf, Abruf am 31.08.2014.

Haas A, Hofmann A (2013) Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. FZID Discussion Paper 74-2013, http://hdl.handle.net/10419/74788

Hallikas J, Virolainen V, Tuominen M (2002) Risk analysis and assessment in network environments: a dyadic case study. International Journal of Production Economics 78(1):45-55

Hallikas J, Karvonen I, Pulkkinen U, Virolainen V, Tuominen M (2004) Risk management processes in supplier networks. International Journal of Production Economics 90(1):47-58

Höfer C, Karagiannis G (2010) Taxonomy of cloud computing services. IEEE GLOBECOM Workshops, Miami, USA

Junginger M (2005) Wertorientierte Steuerung von Risiken im Informationsmanagement. Deutscher Universitäts-Verlag Springer, Wiesbaden

König C, Mette P, Müller HV (2013) Multivendor portfolio strategies in cloud computing. Proceedings of the 21st European Conference on Information Systems (ECIS), Utrecht, Netherlands

Lacity MC, Khan SA, Willcocks LP (2009) A review of the IT outsourcing literature: Insights for practice. The Journal of Strategic Information Systems 18(3):130-146

Lee JN, Huynh MQ, Kwok RCW, Pi SM (2003) IT outsourcing evolution---: past, present, and future. Communications of the ACM 46(5):84-89

Leimeister S, Riedl C, Böhm M, Krcmar H (2010) The business perspective of cloud computing: actors, roles, and value networks. Proceedings of 18th European Conference on Information Systems (ECIS), Pretoria, South Africa

Mell P, Grance T (2011) The NIST Definition of Cloud Computing (Draft). Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland

Miller R (2011) Outage in Dublin Knocks Amazon, Microsoft Data Centers Offline. http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/, Abruf am 31.08.2014.

Neitzke HP (2007) Systemische Risiken. AACCrisk Report 3/2007

Norrman A, Jansson U (2004) Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. International Journal of Physical Distribution & Logistics Management 34(5):434-456

Ojala A, Tyrväinen P (2011) Value networks in cloud computing. Journal of Business Strategy 32(6)40-49

Pelzl N, Helferich A, Herzwurm G (2013) Wertschöpfungsnetzwerke deutscher Cloud-Anbieter. HMD - Praxis der Wirtschaftsinformatik 50(4):42-52

Ritchie B, Brindley C (2007) Supply chain risk management and performance: A guiding framework for future development. International Journal of Operations & Production Management 27(3):303-322

Saripalli P, Walters B (2010) Quirc: A quantitative impact and risk assessment framework for cloud security. Proceedings of the 3rd International Conference on Cloud Computing, Miami, USA

Schließmann CP (2010) Komplexe Systeme brechen wie Glas. Die Bank : Zeitschrift für Bankpolitik und Praxis 6:56-59

Stoneburner G, Goguen A, Feringa A (2001) Risk management guide for information technology systems. National Institute of Standards and Technology Special Publication 800(30)

Tafti (2005) Risks factors associated with offshore IT outsourcing. Industrial Management & Data Systems 105(5):549-560

Trkman P, McCormack K (2009) A conceptual model for managing supply chain risk in turbulent environment. International Journal of Production Economics 119(2):247-258

Troshani I, Rampersad G, Wickramasinghe N (2011) On Cloud Nine? An Integrative Risk Management Framework for Cloud. Proceedings of 24th Bled eConference, Bled, Slovenia

Vaquero LM, Rodero-Merino L, Caceres J, Lindner M (2009) A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer Communication Review 39(1):50-55

Willcocks LP, Lacity MC, Kern T (1999) Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA. Journal of Strategic Information Systems 8(3):285-314

Zhang X, Wuwong N, Li H, Zhang X (2010) Information security risk management framework for the cloud computing environments. Proceedings of the 10th International Conference on Computer and Information Technology, Bradford, UK

Zimmermann S (2008) IT-Portfoliomanagement–Ein Konzept zur Bewertung und Gestaltung von IT. Informatik-Spektrum 31(5):460-468

II Risikoidentifikation und Risikosteuerung in bilateralen IT-Sourcing-Beziehungen

Um Risiken in IT-Sourcing-Netzwerken identifizieren und steuern zu können, ist zunächst das Verständnis von bilateralen IT-Sourcing-Beziehungen notwendig. Daher wird in Kapitel II der Aspekt der Risikoidentifikation und Risikosteuerung zunächst im Kontext von Cloud-Computing-Investitionsentscheidungen und IT-Outsourcing-Projekten betrachtet. Dazu wird in Beitrag 1 eine Strukturierung verschiedener Einflussfaktoren auf Ertrag, Risiko und Abhängigkeiten einer Cloud-Computing-Investition dargestellt, bevor die Auswirkungen verschiedener Gestaltungsspielräume auf diese Faktoren untersucht werden. Mittels der Gestaltungsspielräume, wie beispielsweise der Wahl des Liefermodells oder des Servicemodells, kann die konkrete Ausprägung der Einflussfaktoren im Rahmen der Investition gesteuert werden, wodurch insbesondere auch eine Steuerung der Risiken ermöglicht wird. Beitrag 2 erweitert den Fokus von Cloud-Computing-Investitionen hin zu allgemeinen IT-Outsourcing-Projekten, fokussiert jedoch zugleich auf die konkreten Risiken „Ausfall des IT-Outsourcing-Projektpartners“ und „Vertrauensverlust aufgrund eines Kurzsturzes“, welche beide als Marktrisiken einzuordnen sind. Um diese Risiken steuern zu können, wird ein Ansatz zum Hedging dieser Risiken mittels von Finanzderivaten erarbeitet und anhand eines mathematischen Modells im Detail untersucht. Eine ergänzende Sensitivitätsanalyse behandelt die Fragestellung, wann sich ein solcher Ansatz zur Risikosteuerung aus ökonomischen Gesichtspunkten lohnt und wann andere Steuerungsmechanismen herangezogen werden sollten.

II.1 Beitrag 1: „Gestaltungsspielräume bei Cloud-Computing-Investitionen“[1]

Autor:	Christian König
	Kernkompetenzzentrum Finanz- & Informationsmanagement, Lehrstuhl für BWL, Wirtschaftsinformatik, Informations- & Finanzmanagement (Prof. Dr. Hans Ulrich Buhl) Universität Augsburg, D-86135 Augsburg christian.koenig@fim-rc.de

Erschienen 2014 in:	HMD – Praxis der Wirtschaftsinformatik 51(4):494-505

Zusammenfassung:

Im Rahmen des IT-Portfoliomanagements soll die Gesamtheit der zur Verfügung stehenden IT-Investitionen so koordiniert werden, dass die Unternehmensziele bestmöglich erreicht werden. Durch Cloud Computing als neue Bereitstellungsform für IT-Leistungen existieren dabei verschiedene Handlungsspielräume, über die bei der Planung solcher IT-Investitionen entschieden werden muss. Je nach deren Ausgestaltung ändern sich realisierbare Potenziale von Cloud Computing, aber auch Auszahlungsstruktur und Risiken. Eine optimierte Gestaltung von Cloud-Computing-Investitionen ist nur möglich, wenn die Auswirkungen der jeweiligen Entscheidungen bezüglich der Handlungsspielräume bekannt sind. Diese werden untersucht, strukturiert und in einen Entscheidungsprozess zur Bewertung von Cloud-Computing-Investitionen eingeordnet.

[1] Bei diesem Beitrag handelt es sich um eine redaktionell verbesserte Version des veröffentlichten Beitrags.

II.1.1 Cloud Computing als neue Bereitstellungsform für IT-Leistungen

Cloud Computing als neue Bereitstellungsform für IT-Leistungen lässt sich als konsequente und logische Weiterentwicklung des klassischen IT-Outsourcing-Konzepts begreifen [Böhm et al. 2009, S. 11]. Ausgehend von einem der ersten IT-Outsourcing-Deals im Jahr 1989, als KODAK große Teile der eigenen IT-Infrastruktur an externe Partner, wie beispielsweise IBM, herausgab, bis hin zu heutigen hochflexiblen Angeboten an unterschiedlichsten Services aus der Cloud ist viel passiert. Die grundlegenden Ziele sind dabei gleich geblieben. Unternehmen erhoffen sich durch Sourcing auch in der Cloud weiterhin insbesondere Kostensenkungen, Zugriff auf moderne IT-Ressourcen und Expertenwissen, sowie eine Fokussierung der eigenen Ressourcen auf strategische Ziele (vgl. Lacity et al. [2009, S. 130]). Cloud Computing bietet hierzu einen Pool aus virtualisierten IT-Ressourcen, welche Hardware-, Software- und Entwicklungsplattformservices anbieten. Diese Ressourcen sind einfach zu nutzen und können je nach Bedarf dynamisch skaliert werden, wobei ein nutzungsabhängiges Abrechnungsmodell (pay-per-use) zum Tragen kommt [Vaquero et al. 2009, S. 51]. IT-Lösungen aus der Cloud können hierbei durch eine flexible Unterstützung von Unternehmensprozessen den Anforderungen des Kerngeschäfts Rechnung tragen.

Cloud Computing ist zweifelsfrei ein Mega-Trend in der IT-Branche, sowohl Marktvolumen als auch Datenverkehr sind innerhalb der vergangenen Jahre stetig angestiegen. Die Industrie erwartet auch künftig ein deutliches Wachstum. So schätzt Cisco den weltweiten cloudbasierten Datenverkehr im Jahr 2017 auf 5,3 Zettabytes (Milliarden Terabytes), was einer Vervielfachung um den Faktor 4,5 im Vergleich zum Jahr 2012 entspräche [Cisco 2013, S. 1]. Dabei lassen sich zwei Entwicklungen beobachten.

- Einerseits ist das Produkt „IT-Leistung aus der Cloud“ auf dem Weg zum Commodity, also zu einem verfügbaren Handelsgut. So wurde im Mai 2013 die Deutsche Börse Cloud Exchange AG gegründet mit dem Ziel, eine Handelsplattform für Cloud-basierte, standardisierte IT-Leistungen anzubieten [DBCE 2013]. VMware Solution Exchange bietet ebenfalls einen Online-Marktplatz speziell für Software-as-a-Service-Produkte [VMware 2013]. Solche Plattformen tragen zu erhöhter Transparenz und damit zu einer vereinfachten Handelbarkeit von IT-Leistungen aus der Cloud bei.
- Andererseits ist Cloud Computing nicht immer gleich Cloud Computing. So existieren bei Investitionsvorhaben im Bereich Cloud Computing viele verschiedene Gestaltungsspielräume für den Entscheider, wie beispielsweise die Wahl des Service-

und Liefermodells. Je nach Ausgestaltung solcher Gestaltungsspielräume verändern sich die Potenziale und die Risiken.

Im Unternehmen müssen Cloud-Computing-Investitionsentscheidungen im Rahmen des IT-Portfoliomanagements geplant werden. Dabei sind die Grundsätze der IT-Governance zu berücksichtigen, welche sicherstellen, dass IT-Investitionen in Einklang mit dem Ziel der wertorientierten Unternehmensführung getroffen werden. Das bedeutet insbesondere, dass der Unternehmenswert gesteigert werden soll, während die dabei einzugehenden Risiken und existierende Abhängigkeiten Betrachtung finden [Zimmermann 2008, S. 461 f.]. Der Wertbeitrag eines betrachteten IT-Bewertungsgegenstands sollte dabei anhand eines monetären Werts gemessen werden, welcher im Folgenden als Ertrag bezeichnet wird und auf Zahlungsströmen basiert. Neben dem Ertrag, der bei der ex-ante Planung von IT-Investitionen zumeist nur einen erwarteten Betrag widerspiegeln kann, sind vorhandene Risiken bezüglich dessen Realisierung zu berücksichtigen. Des Weiteren dürfen einzelne Investitionen nicht isoliert betrachtet werden. Gesamtwert und -risiko des IT-Portfolios sind maßgeblich von den Beziehungen zwischen den einzelnen IT-Bewertungsgegenständen abhängig.

II.1.2 Strukturierung der Gestaltungsspielräume

Ein IT-Bewertungsgegenstand bei Cloud-Computing-Investitionen kann entweder ein konkreter Cloud-Service sein, oder aber ein Projekt zum Bezug verschiedener IT-Services aus der Cloud. Dabei kommen die Charakteristika von Cloud Computing zum Tragen, welche in verschiedenen Fällen von den bisher üblichen IT-Investitionen abweichen. Im Folgenden wird angelehnt an die Arbeit von Zimmermann [2008] eine Strukturierung in die folgenden vorhandenen Gestaltungsspielräume vorgeschlagen:

- *Flexibilität des Liefermodells*
- *Flexibilität des Servicemodells*
- *zeitliche Flexibilität*

Diese Spielräume bestehen sowohl zum Investitionszeitpunkt als auch während der Laufzeit und ermöglichen die Einflussnahme auf die Ertrags-/Risikoposition der Cloud-Computing-Investitionen.

Der Begriff *Flexibilität des Liefermodells* bezeichnet den vorhandenen Gestaltungsspielraum zwischen einer „klassischen“ Public Cloud, einer Private Cloud und der Zwischenlösung in Form einer Hybrid Cloud. Aufgrund der Eigenschaft des Bezugs der Cloud-Services über ein

Netzwerk wird klar, dass hier im Gegensatz zum IT-Outsourcing keine räumliche, sondern die organisatorische Dimension der Ausgestaltung von Bedeutung ist.

Der Begriff *Flexibilität des Servicemodells* bezeichnet den vorhandenen Gestaltungsspielraum bei der Wahl der Art des Services. Dieser kann Infrastruktur- (IaaS), Plattform- (PaaS), oder Software-Dienste (SaaS) erfüllen und ist als eine „Black-Box" zu verstehen, die eine bestimmte Funktionalität bereitstellt. Es ist dabei zu entscheiden, ob Cloud-Services bloße IT-Infrastruktur oder Plattformen liefern sollen, auf denen dann möglicherweise eigene Applikationen aufgesetzt werden, oder ob die gewünschte Software direkt als SaaS bezogen und genutzt werden soll. Die Nutzung von IaaS-Diensten lässt aufgrund höherer Homogenität eine vergleichsweise einfachere Kombination verschiedener Dienste zu. So können beispielsweise Cloud-Services wie Datenspeicher oder Recheninstanzen miteinander interagieren und aufgrund standardisierter Schnittstellen und Dateiformate gemeinsame Daten verarbeiten und weiterreichen. Dahingegen ist SaaS tendenziell spezialisierter und bietet daher weniger Einflussnahme. Zudem kann bei komplexeren Services wie SaaS in aller Regel kein Einfluss auf die darunter liegenden Infrastrukturen genommen werden.

Der Begriff der *zeitlichen Flexibilität* beschreibt Handlungsoptionen, die während der Lebensdauer des IT-Bewertungsgegenstands bestehen. Bei Cloud-Computing-Investitionen wird dabei deutlich, dass – wenn auch teilweise abhängig von Liefer- und Servicemodell – eine hohe Handlungsflexibilität besteht, die zu nahezu jedem Zeitpunkt äußerst kurzfristig und unkompliziert eine Ausweitung (Investition), eine Verringerung oder gar einen Abbruch (Desinvestition), und damit auch eine Umstrukturierung des bestehenden Cloud-Service-Portfolios ermöglicht.

Diese Dimensionen im Rahmen von Cloud-Computing-Investitionen können in Anlehnung an die Darstellung von Zimmermann [2008] strukturiert werden (Abb. II-1).

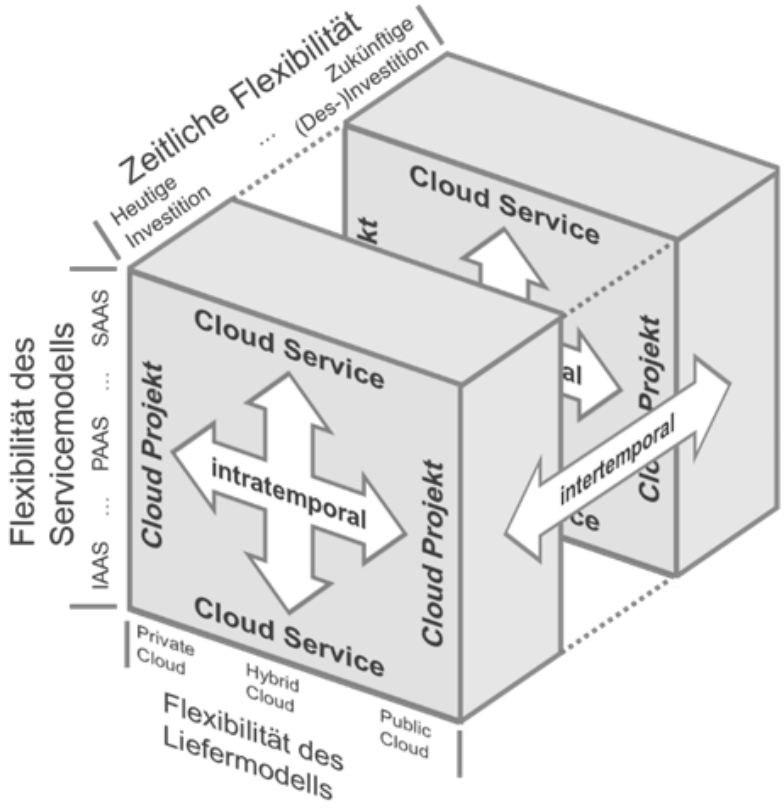

Abb. II-1 Handlungsspielräume bei Cloud-Computing-Investitionen

II.1.3 Auswirkungen auf Ertrag, Risiko und Komplexität

Es ist Aufgabe des IT-Portfoliomanagements, IT-Investitionen so zu gestalten, dass sich Ertrag und Risiko der Cloud-Investition bestmöglich im Sinne des Unternehmens auswirken. Hierzu müssen die nicht immer direkt ersichtlichen Auswirkungen der vorhandenen Gestaltungsspielräume von Cloud-Computing-Investitionen bekannt sein. Dadurch lassen sich in der Praxis die ökonomischen Effekte der Investitionen leichter abschätzen.

Zhang et al. [2010] beschreiben verschiedene Benefits, die bei der Adaption von Cloud Computing resultieren und die Ertragsposition des Unternehmens beeinflussen. Armbrust et al. [2010] diskutieren mögliche Hindernisse und Risiken, die im Rahmen des Einsatzes von Cloud Computing existieren und sich auf die Risikoposition des Unternehmens auswirken können. Darauf aufbauend wird im Folgenden eine Übersicht (Tab. II-1) an möglichen Einflussfaktoren gegeben, die sich letztendlich im Wertbeitrag der Investition manifestieren. Anschließend wird exemplarisch beschrieben, wie sich Entscheidungen bezüglich der Gestaltungsspielräume mittels dieser Einflussfaktoren tendenziell auf Ertrag, Risiko und Komplexität der Investition auswirken. Einflussfaktoren auf die Ertragsposition des Unternehmens können sich dabei direkt

oder indirekt auswirken. Das Risiko stellt sich als Abweichung vom erwarteten Ertrag dar und wird von vorhandenen Abhängigkeiten beeinflusst, die dabei die Komplexität der Cloud-Computing-Investition erhöhen.

Einflussfaktor	*Beschreibung*	*Auswirkung auf*
Höhe der Investitionsauszahlungen	direkte Wirkung	Ertrag
Höhe der Auszahlungen für den operativen Betrieb	direkte Wirkung	Ertrag
Höhe der Auszahlungen für Wartung	direkte Wirkung	Ertrag
Höhe der Auszahlungen zur Schaffung und zum Betrieb von Schnittstellen	direkte Wirkung	Ertrag
Ad-hoc Verfügbarkeit von zusätzlicher IT-Kapazität	indirekte Wirkung über bspw. Steigerung des Umsatzes	Ertrag
Möglichkeit zur ad-hoc Umgestaltung der IT	indirekte Wirkung über bspw. Vermeidung drohenden Verlusts oder Abschöpfung zus. Kundenpotenzials	Ertrag
Temporärer Ausfall der IT	- Ursache bspw. technische Probleme am Standort des Cloud-Providers oder auf dem Übertragungsweg - Kurzfristige Unterbrechung der abhängigen Geschäftsprozesse	Risiko
Dauerhafter Ausfall der IT	- Ursache bspw. Insolvenz des Cloud-Providers - Mittel- bis langfristige Unterbrechung der abhängigen Geschäftsprozesse, Anbietersuche, Migration	Risiko
Datensicherheit und Datenschutz	- Verlust oder ungewünschte Weitergabe von Unternehmensdaten kann Geschäftsmodell stark beeinträchtigen - Fehlende Einhaltung von Datenschutzrichtlinien führt bspw. zu Strafzahlungen und negativer Außenwirkung	Risiko
Lock-In	- Erschwerter Wechsel vom aktuellen Cloud-Provider zu einem anderen Anbieter - Gefahr von Preissteigerungen	Risiko
Inkompatibilitäten durch anbieterseitige Updates	- Auszahlungen zur Wiederherstellung der Kompatibilität notwendig - Andernfalls suboptimale Unterstützung des Geschäftsmodells	Risiko
Intratemporale ressourcenorientierte Abhängigkeiten	Limitierte interne Ressourcen zu einem bestimmten Zeitpunkt, wie bspw. maximale Bandbreite	Komplexität
Intratemporale strukturelle Abhängigkeiten	Strukturelle Gegebenheiten zu einem bestimmten Zeitpunkt, wie bspw. gegenseitiger Zugriff v. Cloud-Services	Komplexität
Intertemporale Abhängigkeiten	Abhängigkeiten zwischen Investitionszeitpunkt und zukünftigem Zeitpunkt, wie bspw. heutige Basisinvestitionen und resultierende Einschränkungen in Zukunft	Komplexität

Tab. II-1 Einflussfaktoren auf den Wertbeitrag

II.1.3.1 Exemplarische Auswirkungen der Flexibilität des Liefermodells

Im Rahmen der *Public Cloud* ergeben sich große Einsparungen bei den Investitionsauszahlungen, da hier keine eigene Infrastruktur vorgehalten werden muss. Bezüglich Datensicherheit und Datenschutz besteht durch das Herausgeben der Verantwortung ein hohes Risiko, zudem liegen die Daten möglicherweise in einem anderen Rechtsraum. Ressourcen wie Hardwarekomponenten oder IT-Administratoren sind nicht zu stellen, jedoch ist hier unter Umständen die zur Verfügung stehende Bandbreite zu beachten, die bei hoher Nachfrage einen Flaschenhals darstellen kann. Die ressourcenorientierte Abhängigkeit ist damit als relativ gering einzuschätzen. Bei einer *Private Cloud* müssen Services zunächst bereitgestellt werden, was in ähnlichem Umfang wie bei einem klassischen Rechenzentrum mit hohen Investitionsauszahlungen einhergeht. Dafür kann die Datenhaltung als vergleichsweise sicher angesehen werden, da Unternehmens- oder Kundendaten vor unbefugtem Zugriff geschützt auf eigenen Datenspeichern abgelegt sind. Ressourcenorientierte Abhängigkeiten sind als hoch zu bewerten, da die benötigten Ressourcen für alle Cloud-Services ausreichend bereitgestellt werden müssen. Eine *hybride Lösung* bedarf ebenso Investitionsauszahlungen für den privaten Teil der Cloud, jedoch muss die Hardware nicht immer für die maximal denkbare Auslastung kalkuliert werden, da ab einer bestimmten Nachfrage auf Public-Cloud-Leistungen zugegriffen wird. Datenschutzrisiken können größtenteils ausgeschlossen werden, insofern sensitive Daten im privaten Teil der Cloud vorgehalten werden. Die ressourcenorientierte Abhängigkeit ist bei Hybrid Cloud als relativ gering einzuschätzen, da im Zweifelsfall auf externe Cloud-Services zugegriffen werden kann. Zusammenfassend lässt sich festhalten:

- Eine Verlagerung in die Public Cloud wirkt sich insbesondere positiv auf die Ertragsposition aus, birgt jedoch gleichzeitig ein hohes Maß an Risiken.
- Eine Private Cloud fängt die meisten Cloud-Computing-spezifischen Risiken auf, ermöglicht aber nahezu keine der erhofften Vorteile und erscheint deswegen nur bei sehr hoher Risikoaversion angemessen.
- Eine Hybrid Cloud als Mischlösung stellt einen guten Kompromiss dar um Vorteile wie Flexibilität und Kostenreduktion zumindest teilweise zu realisieren und gleichzeitig die einhergehenden Risiken beherrschbar zu machen. Dabei muss jedoch eine erhöhte Komplexität in Kauf genommen werden.

II.1.3.2 Exemplarische Auswirkungen der Flexibilität des Servicemodells

Aufgrund hoher Homogenität und niedriger Komplexität ermöglichen *Infrastrukturdienste* eine relativ einfache ad-hoc Umgestaltung der IT in Form eines Austausches funktionsgleicher oder kompatibler Services und weisen ein geringes Risiko bezüglich eines Ausfalls auf, da sie zudem oftmals von großen etablierten Anbietern wie Amazon oder Google bereitgestellt werden. Dabei sind sie mit nur wenigen strukturellen Abhängigkeiten behaftet, was ein einfaches Zusammenspiel verschiedener Services untereinander gestattet. Während *Plattformdienste* aus ähnlichen Gründen ebenfalls eine tendenziell einfache ad-hoc Umgestaltung der IT erlauben und noch handhabbare strukturellen Abhängigkeiten aufweisen, muss sowohl das Risiko eines temporären als auch eines dauerhaften Ausfalls der Cloud-Services im Vergleich zu Infrastrukturdiensten als höher angesehen werden, da Plattformdienste wiederum auf diesen basieren und technische Probleme daher an mehreren Stellen der Leistungserstellung auftreten können. Bei *Softwarediensten* ist eine Neugestaltung der Servicelandschaft aufgrund der höheren Komplexität als vergleichsweise schwer anzusehen, wobei zudem noch die Problematik besteht, am Markt die passenden spezialisierten Services zu finden. Dies wirkt sich ebenfalls auf die demnach als hoch einzuschätzenden strukturellen Abhängigkeiten aus. Das Ausfallrisiko ist aufgrund verschiedener zugrunde liegenden Services ebenfalls als hoch anzusehen und die erhöhte Komplexität und Spezialisierung von SaaS führen dazu, dass diese – abgesehen von wenigen hochentwickelten und weitverbreiteten Services wie beispielsweise Microsoft Office 365 – tendenziell von kleineren spezialisierten Anbietern erbracht werden, die eine höhere Unsicherheit bezüglich ihres langfristigen Fortbestehens aufweisen. Es lässt sich festhalten:

- Die Auswirkungen von Entscheidungen bezüglich der Flexibilität des Servicemodells hängen zumeist von der Homogenität des betrachteten Services ab.
- SaaS führt tendenziell zu höheren Auszahlungen, weist höhere Risiken auf und verursacht mehr Komplexität als IaaS und PaaS.
- In Zukunft ist mit einer zunehmenden Standardisierung auch solcher Services zu rechnen, was tendenziell zu einer Abschwächung der beschriebenen Probleme führen wird.

II.1.3.3 Exemplarische Auswirkungen der zeitlichen Flexibilität

Neben den Entscheidungen zum Investitionszeitpunkt bestehen auch während der Laufzeit mittels Einflussnahme durch zusätzliche *Investition* oder *Desinvestition* umfangreiche

Handlungsflexibilitäten. Sind stand heute (2014) bestimmte Anforderungen an Cloud-Services noch unsicher, so kann deren Bezug problemlos aufgeschoben werden. Sind die Anforderungen geklärt oder neue Umstände eingetreten, so können die benötigten Cloud-Services kurzfristig bezogen werden. Ebenso können nicht mehr benötigte Services ohne weitere Verpflichtungen eingestellt werden. Dabei werden insbesondere Auszahlungen für Investitionen und Wartung eingespart. Durch eine Desinvestition bei Cloud-Services von „problematischen" Anbietern können die entsprechenden Risiken verringert werden, insofern solche Entwicklungen rechtzeitig erkannt werden. Hierbei kann es sich um Anbieter handeln, die beispielsweise vermehrt mit technischen Problemen zu kämpfen haben, sich in finanzieller Schieflage befinden oder beim Thema Datensicherheit oder Datenschutz negative Schlagzeilen machen. Ebenso sind einmal zu Beginn festgelegte Kapazitäten und Strukturen nicht für die gesamte Laufzeit fixiert. Durch eine spätere Anpassung der Cloud-Services kann eine intertemporale Abhängigkeit relativ einfach aufgelöst werden. Damit fällt beispielsweise die Notwendigkeit weg, reine Basisinvestitionen als Grundlage für künftige Erweiterungen durchzuführen oder sich frühzeitig auf einen bestimmten Anbieter festlegen zu müssen. Damit bleibt festzuhalten:

- Durch das Ausnutzen der zeitlichen Flexibilität ist eine positive Einflussnahme auf Ertrag, Risiko und Komplexität der Investition möglich, der Entscheider kann die Investition anpassen, muss aber nicht.
- Um solche Vorteile realisieren zu können ist jedoch eine dauerhafte Beobachtung sowie ein aktives Gestalten der Cloud-Investition notwendig. Eine reine hochautomatisierte Selbstverwaltung der Cloud-Services, die beispielsweise selbstständig Kapazitäten erhöhen und verringern kann, greift daher zu kurz.

Über diese exemplarische Betrachtung hinaus gibt Tabelle Tab. II-2 eine Einschätzung bezüglich der Richtung (Pfeile von oben nach unten: positiv, eher positiv, neutral, eher negativ, negativ), sowie eine Bewertung der Vorteilhaftigkeit der Auswirkungen auf Ertrag, Risiko und Komplexität (Schattierung von hell zu dunkel: vorteilhaft, eher vorteilhaft, neutral, eher nachteilig, nachteilig) der Cloud-Investition wieder.

		Flexibilität des Liefermodells			Flexibilität des Servicemodells			Zeitliche Flexibilität
		Public	Hybrid	Private	IaaS	PaaS	SaaS	zukünftige (Des-)Investition
Auswirkung auf Ertrag	*Einsparungen bei Investitionsauszahlungen*	↑	↘	↓	-	-	-	↗
	Einsparungen bei Auszahlungen für den operativen Betrieb	↗	→	↘	-	-	-	-
	Einsparungen bei Auszahlungen für Wartung	↑	↘	↓	-	-	-	↗
	Einsparungen bei Auszahlungen zur Schaffung und zum Betrieb von Schnittstellen	↗	↓	↑	↗	→	↘	-
	Generierung von Einzahlungen durch ad-hoc Verfügbarkeit von zusätzlicher IT-Kapazität	↑	↑	↓	-	-	-	↑
	Vermeidung von Auszahlungen / Generierung von Einzahlungen durch Möglichkeit zur ad-hoc Umgestaltung der IT	↑	→	↘	↑	↗	↘	↑
Auswirkung auf Risiko	*Temporärer Ausfall der IT*	↑	↓	→	↘	→	↗	↘
	Dauerhafter Ausfall der IT	↑	→	↓	↘	→	↗	↘
	Datensicherheit und Datenschutz	↑	↘	↓	-	-	-	↘
	Lock-In	↑	→	↓	↘	→	↗	-
	Inkompatibilitäten durch anbieterseitige Updates	↘	↑	↓	↓	↗	↑	-
Auswirkung auf Komplexität	*Intratemporale ressourcenorientierte Abhängigkeiten*	↘	↘	↗	-	-	-	-
	Intratemporale strukturelle Abhängigkeiten	→	↑	↘	↘	→	↑	-
	Intertemporale Abhängigkeiten	↓	↗	↑	↓	↘	↗	↓

Tab. II-2 Auswirkungen der Gestaltungsspielräume

II.1.4 Darstellung eines Entscheidungsprozesses für Cloud-Computing-Investitionen anhand eines Fallbeispiels

Um Cloud-Computing-Investitionsentscheidungen fundiert treffen zu können empfiehlt es sich, anhand eines strukturierten Entscheidungsprozesses vorzugehen. Hierzu bietet sich die Anpassung des allgemeinen Entscheidungsprozesses nach Kruschwitz [2007, S. 7 ff.] an. Dazu werden im Folgenden die adaptierten Phasen Problemstellungsphase, Suchphase, Beurteilungsphase, Entscheidungsphase, Realisierungsphase und Kontrollphase kurz vorgestellt und anhand eines realen Fallbeispiels verdeutlicht.

In der *Problemstellungsphase* wird die Ausgangslage analysiert und die Idee geboren, die bestehenden Anforderungen mittels einer Cloud-Computing-Investition zu erfüllen. Im konkreten Fall handelt es sich um eine Organisation mit ca. 150 Mitarbeitern, die angewandte Forschungsprojekte durchführt und ein ähnliches Anforderungsprofil wie eine Unternehmensberatung aufweist. Dies geschieht verteilt auf drei feste Standorte sowie mehrere wechselnde Projektstandorte. Die festen Standorte sind durch einen Zusammenschluss

kleinerer Forschungseinheiten entstanden und weisen eine heterogene, teilvirtualisierte IT-Landschaft auf. Dabei sind die Standorte teilweise in die Netzwerke von Universitäten mit unterschiedlichen Benutzerverwaltungen eingebunden. Diese komplexe Infrastruktur wird von dezentralen Teams aus Mitarbeitern und Teilzeitkräften betreut. Mittels verschiedener Eigenentwicklungen kann zumindest eine grundlegende Zusammenarbeit zwischen den Standorten ermöglicht werden. Server für die Verwaltung von Kalendern und Kontakten werden eigens betrieben, wohingegen E-Mails über die verschiedenen Rechenzentren der Universitäten abgewickelt werden. Daten werden auf Servern der Rechenzentren, mangels ausreichender Kapazität aber teilweise auch selbst gespeichert, wobei unterschiedliche Backup-Strategien verwendet werden. Da an allen Standorten kontinuierlich neue Mitarbeiter eingestellt werden und eine Ausweitung auf weitere Standorte für die nahe bis mittlere Zukunft angestrebt wird, steht die Organisation vor der Herausforderung, eine standortunabhängige, einfach zu wartende und flexibel skalierbare IT-Unterstützung bereitzustellen und möchte dies mit einer Cloud-Computing-Lösung umsetzen. Im Fokus der Betrachtung stehen dabei der Bezug von Mail, Kalender und Kontakten (Exchange) und eine zentrale Datenhaltung inkl. Abwicklung des externen und internen Webauftritts (Sharepoint).

In der *Suchphase* sind Handlungsmöglichkeiten und deren Konsequenzen zu ermitteln. Dazu werden Prognoseverfahren benötigt um Aussagen über künftige Entwicklungen treffen zu können. Hier bietet sich die Betrachtung der vorhandenen Flexibilitäten einer Cloud-Computing-Investition an (siehe Abb. II-1), um sowohl Gestaltungsspielräume und damit mögliche Entscheidungsalternativen, als auch grundsätzliche Auswirkungen dieser abschätzen zu können.

- Alternative A1: Eigene Bereitstellung der Dienste mittels IaaS und darauf installierter Software im Rahmen einer Private Cloud
- Alternative A2: Fremdbezug der Dienste mittels SaaS im Rahmen einer Public Cloud

In der *Beurteilungsphase* werden die gefundenen Handlungsmöglichkeiten quantitativ und/oder qualitativ bewertet und anschließend verknüpft. Hierzu können die vorgestellten Einflussfaktoren auf Ertrag, Risiko und Komplexität (siehe Tab. II-1) als Strukturierungshilfe herangezogen werden, um eine Bewertung aller Auswirkungen der jeweiligen Handlungsmöglichkeit vollumfänglich sicher zu stellen.

Konkret wurden beide Alternativen soweit möglich quantitativ (gesamte Auszahlungen im Planungszeitraum (5 Jahre); gerundete, wenn nötig geschätzte Werte), sonst qualitativ

(Scoring-Wert SW, 1 = sehr gut bis 5 = sehr schlecht) bewertet und anschließend in jedem der drei Bereiche mit einem Rangwert belegt, um einen Vergleich zu ermöglichen.

Als Investitionsauszahlungen fallen bei A1 Auszahlungen zur Anschaffung eines eigenen leistungsstarken Servers, der auch zukünftige Nachfragen bedienen müsste, und der benötigten Software bei A1 an, sowie bei beiden Alternativen unterschiedliche Auszahlungen für Installation und Einrichtung durch eigene Mitarbeiter (A1: ca. 48.000 EUR / A2: ca. 3.000 EUR). Bezüglich der Auszahlungen für den operativen Betrieb stellen die hohen laufenden Lizenzgebühren bei A2 den einzigen Posten dar, da im betrachteten Fall die Stromkosten bei Alternative A1 nicht selbst zu tragen sind, was im Allgemeinen jedoch berücksichtigt werden sollte (A1: 0 EUR / A2: ca. 32.000 EUR). Auszahlungen für die Wartung sind beim Eigenbetrieb (A1) deutlich höher einzuschätzen als beim Fremdbezug der Services (A2), da bei letzterem die Fehlersuche und Behebung als auch das Einspielen von Updates seitens der eigenen Mitarbeiter entfällt (A1: ca. 24.000 EUR / A2: ca. 6.000 EUR). Dabei ist auch zu beachten, dass im Vergleich zu A2 bei A1 im betrachteten Zeitraum keine kostenfreien Aktualisierungen beinhaltet sind. Auszahlungen zur Schaffung und zum Betrieb von Schnittstellen sind bei beiden Alternativen nicht zu berücksichtigen, da es sich um eine Standardsoftware handelt, die in beiden Implementierungsvarianten mit der restlichen Infrastruktur vollständig kompatibel ist. Die ad-hoc Verfügbarkeit von zusätzlicher IT-Leistung wird qualitativ bewertet und schneidet bei A1 schlechter ab als bei A2, da bei letzterer das Zuschalten weiterer Benutzerkonten sehr einfach und kurzfristig möglich ist, so dass neue Mitarbeiter schnell produktiv arbeiten können, wohingegen im ersten Fall eine aufwändigere Konfiguration notwendig ist und gegebenenfalls die Hardware erweitert werden muss (A1: SW 5 / A2: SW 1). Eine Umgestaltung der gewählten Struktur ist bei beiden Alternativen nicht ohne weiteres möglich (A1: SW 3 / A2: SW 3). Zusammenfassend ergeben sich Auszahlungen für A1 in Höhe von 72.000 EUR, für A2 in Höhe von 41.000 EUR, oder eine Ersparnis durch A2 von 43 % im Vergleich zu A1. Unter Berücksichtigung der zusätzlichen Scoring-Werte ergibt sich für die Ertragsbetrachtung die Rangfolge $A1 \prec A2$.

Das Risiko eines temporären Ausfalls wird für A1 etwas höher bewertet als bei A2, da seitens des externen Anbieters eine deutlich höhere Expertise bezüglich des Betriebs des Cloud-Services zu erwarten ist (A1: SW 4 / A2: SW 2). Das Risiko eines dauerhaften Ausfalls kann für A1 aufgrund Eigenbetrieb als nicht relevant angesehen werden und erscheint auch bei A2 als sehr gering, da es sich dabei um einen etablierten sehr großen Anbieter handelt (A1: SW 1 / A2: SW 2). In Bezug auf das Datenschutz- und Datensicherheitsrisiko einer Public Cloud (A2)

wird im konkreten Fall die Gefahr böswilligen fremden Zugriffs aufgrund der Ausrichtung der Organisation als gering erachtet. Zudem besteht seitens des externen Anbieters eine deutlich professionellere Absicherung der Daten mit entsprechenden Regelungen zum Datenschutz als dies seitens der Organisation selbst zu leisten ist, wobei bei A1 immer noch physischer Zugriff auf die Infrastruktur möglich ist (A1: SW 3 / A2: SW 3). Da das verwendete Produkt vom gleichen Hersteller ist, ist das Lock-In-Risiko in beiden Fällen als relativ hoch anzusehen, ein Wechsel zu einer anderen Software ist hier grundsätzlich aber möglich (A1: SW 4 / A2: SW 4). Inkompatibilitäten durch Updates sollten einerseits (A1) durch Eigenbetrieb ausgeschlossen werden, andererseits aufgrund der sehr hohen Verbreitung der Public-Cloud-Variante (A2) unkritisch sein (A1: SW 1 / A2: SW 2). Da beim Vergleich der Scoring-Werte für den Entscheider das Hauptaugenmerk auf der Verfügbarkeit des Cloud-Services liegt, ergibt sich für die Risikobetrachtung ein leichter Vorteil für A2 und damit die Rangfolge $A1 \prec A2$.

Eine ressourcenorientierte Abhängigkeit stellen bei A1 die verfügbare Hardware und die für Wartung und Fehlerbehebung zuständigen Mitarbeiter dar. Diese beiden Themen können bei A2 als unkritisch betrachtet werden, hier ist ausschließlich die genutzte Bandbreite zu beachten (A1: SW 4 / A2: SW 2). Bezüglich struktureller Abhängigkeiten ist bei A1 und A2 zu beachten, dass die verschiedenen Dienste gebündelt bereitgestellt werden und demnach im Falle eines Ausfalls auch komplett betroffen wären (A1: SW 3 / A2: SW 3). Intertemporale Abhängigkeiten sind bei A1 in Form der zum Investitionszeitpunkt erfolgenden Bestimmung der notwendigen Kapazität vorhanden, welche künftige Anpassungen erschwert. Dies ist bei A2 als unkritisch zu sehen (A1: SW 4 / A2: SW 1). Demnach ergibt sich für die Komplexitätsbetrachtung die Rangfolge $A1 \prec A2$.

In der *Entscheidungsphase* wird die zu realisierende Alternative durch Vergleich der beurteilten Handlungsmöglichkeiten anhand gängiger Entscheidungsregeln bestimmt. Im vorgestellten Fall wurden die ermittelten Rangfolgen der beiden Alternativen A1 und A2 verglichen, woraus die Entscheidung zur Durchführung von A2 folgte, da A1 in allen betrachteten Bereichen von A2 dominiert wird. Dies entspricht dem Bezug der Cloud-Services Mail, Kalender und Kontakten, sowie Datenhaltung inkl. Abwicklung des externen und internen Webauftritts (Microsoft Office 365 und Sharepoint) per Software as a Service aus einer Public Cloud. Je nach Projektumfang könnte darüber hinaus insbesondere die Verrechnung der Scoring-Werte durch die Einführung von Gewichtungen zwischen den einzelnen Einflussfaktoren verbessert werden. Zudem ist es auch denkbar, für die Risiko- und Komplexitätsbestimmung anspruchsvollere quantitative Verfahren zu verwenden.

In der *Realisierungsphase* wird die Investition anschließend in die Tat umgesetzt, was dem Bezug der gewählten Cloud-Services entspricht. Dabei ist die im Vergleich zu klassischen IT-Investitionen relativ kurze Anbahnungsphase zu beachten, die eine schnellere Produktivsetzung ermöglicht.

In der *Kontrollphase* wird der Vergleich zwischen den erwarteten und den tatsächlichen Konsequenzen gezogen. Im Rahmen von Cloud-Computing-Investitionen ist dabei insbesondere die zeitliche Flexibilität zu beachten, das heißt die Möglichkeit zur Anpassung des bestehenden Cloud-Service-Portfolios, um gezogene Schlussfolgerungen und Korrekturen innerhalb der Kontrollphase kurzfristig in die Tat umzusetzen.

II.1.5 Literatur

[Armbrust et al. 2010] *Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A. D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M.*: A view of cloud computing. Communications of the ACM 53 (2010), 4, p. 50-58.

[Böhm et al. 2009] *Böhm, M.; Leimeister, S.; Riedl, C.; Krcmar, H.*: Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen. Information Management & Consulting 24 (2009), 2, p. 6-14.

[Cisco 2013] *Cisco*: Global Cloud Index, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf; Zugriff am 29.01.2014.

[DBCE 2013] *Deutsche Börse Cloud Exchange AG*: Wer wir sind, http://dbcloudexchange.com/de-de/uberuns; Zugriff am 29.01.2014.

[Kruschwitz 2007] *Kruschwitz, L.*: Investitionsrechnung. Oldenbourg Wissenschaftsverlag, München, 2007.

[Lacity et al. 2009] *Lacity, M. C.; Khan, S. A.; Willcocks, L. P.*: A review of the IT outsourcing literature: Insights for practice. The Journal of Strategic Information Systems 18 (2009), 3, p. 130-146.

[Vaquero et al. 2008] *Vaquero, L. M.; Rodero-Merino, L.; Caceres, J.; Lindner, M.*: A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review 39 (2008), 1, p. 50-55.

[VMware 2013] *VMware Solution Exchange*: Learn more about the VMware Solution Exchange, https://solutionexchange.vmware.com/store/content/vsx-learn-more; Zugriff am 09.12.2013.

[Zhang et al. 2010] *Zhang, Q.; Cheng, L.; Boutaba, R.*: Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1 (2010), 1, p. 7-18.

[Zimmermann 2008] *Zimmermann, S.*: IT-Portfoliomanagement–Ein Konzept zur Bewertung und Gestaltung von IT. Informatik-Spektrum, 31 (2008), 5, p. 460-468.

II.2 Beitrag 2: „Using Financial Derivatives to Hedge Against Market Risks in IT Outsourcing Projects – a Quantitative Decision Model“[2]

Autoren:	Hans Ulrich Buhl, Gilbert Fridgen, Christian König Kernkompetenzzentrum Finanz- & Informationsmanagement, Lehrstuhl für BWL, Wirtschaftsinformatik, Informations- & Finanzmanagement (Prof. Dr. Hans Ulrich Buhl) Universität Augsburg, D-86135 Augsburg {hans-ulrich.buhl, gilbert.fridgen, christian.koenig}@fim-rc.de
Erschienen 2013 in:	Journal of Decision Systems 22(4):249-264

Zusammenfassung:

Besides the project-inherent risk of an IT outsourcing project, related to the management of the project, other types of risk driven by the markets have not yet been addressed until now. Although financial derivatives are well known as a powerful tool for hedging market risk, there are no approaches to utilize this tool for risk management in IT outsourcing projects. We show a way to address two types of market risk threatening outsourcing success: insolvency of the project counterpart and a slump in prices of the counterpart's stocks. This paper therefore provides a quantitative decision model to determine how much money should be spent on hedging these risks using financial derivatives. We discover that the lower the probability of damage the higher the degree of cheap hedging that should be applied. In contrast, other means of hedging should be considered when facing a rather high probability of damage, because financial hedging gets too expensive.

[2] This is an Accepted Manuscript of an article published by Taylor & Francis in Journal of Decision Systems on 15 Oct 2013, available online: http://www.tandfonline.com/10.1080/12460125.2013.834680.

II.2.1 Introduction

Despite winning an "Outsourcing Excellence Award" together with Wipro in 2007 (Business Wire India, 2007), the Canadian telecommunication equipment manufacturer Nortel filed for bankruptcy only two years later in 2009 (CBC News, 2009). From 2000, the breakdown of Baan (Baker, Spiro, & Hamm, 2000) made many of their clients overthink their outsourcing strategy and change to other providers. In general, an IT outsourcing provider and its client face several risks when agreeing on an IT outsourcing contract. Besides all the project-inherent risks that occur within an IT outsourcing project, the client could expect that it would suffer financial damage if the service provider suddenly became insolvent and wasn't able to continue the ongoing IT outsourcing project. On the other hand, the service provider might also be concerned about a possible heavy slump in the client's stock price. This would not necessarily lead to the client's insolvency, but it's possible that the resulting pressure on its management might negatively affect the IT outsourcing project and eventually lead to financial damage for the service provider. Furthermore, the case of a client filing for bankruptcy and a service provider suffering a heavy slump in prices might also be conceivable. Figure Abb. II-2 exemplarily illustrates the two types of risk analyzed in this paper.

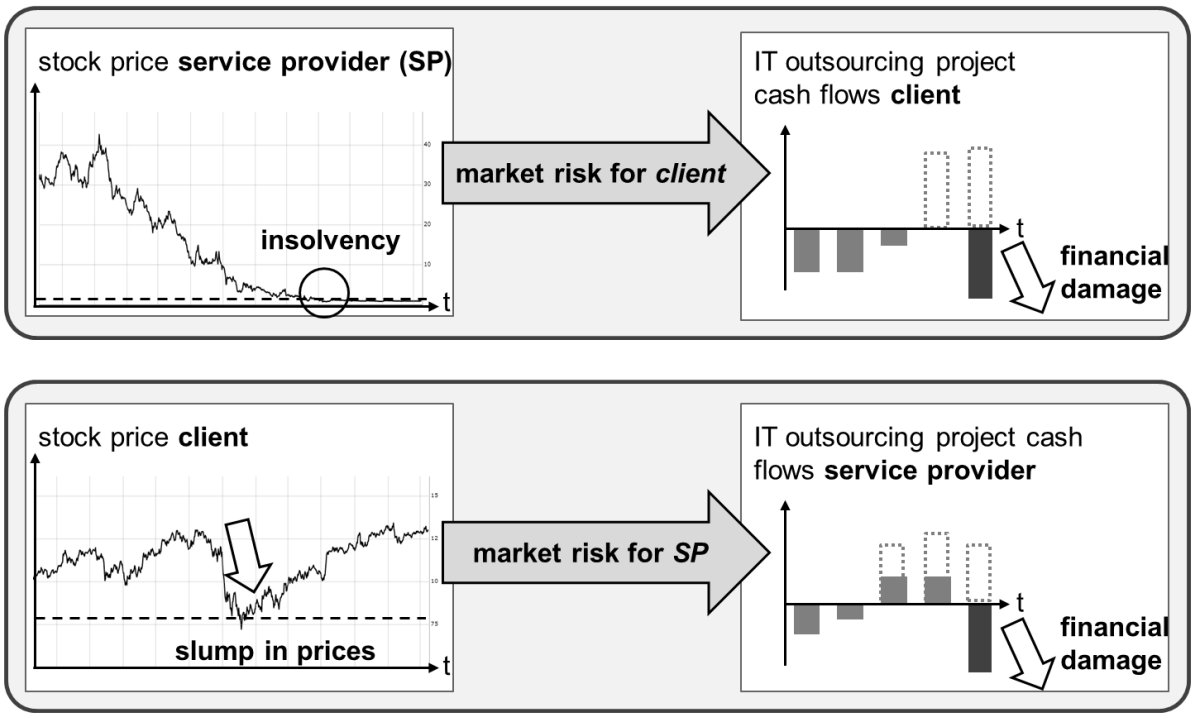

Abb. II-2 Market Risk Causes Financial Damage to IT Outsourcing Partners

Both types of risk in IT outsourcing projects, insolvency of the project partner and a heavy slump in the project partner's stock price, are induced by the markets and can lead to enormous financial damage. As budgets for IT outsourcing projects are rising, the possible damage in case of IT outsourcing failure rises, too. Especially IT outsourcing projects suffer from very high switching costs when trying to transfer unfinished customer tailored projects from one service provider to another. These costs have to be shouldered when being forced to cancel a failed IT outsourcing relationship due to an insolvent project partner. Feeny & Willcocks (1998) name substantial switching cost "the single most threatening aspect of IS/IT outsourcing" (p. 15). Furthermore, a heavy slump in prices of the project partner's stocks, on the one hand, might contingently lead to increased cost pressure, resulting in budget cuts or even (sub-)project cancellations, and, on the other hand, could eventually provoke changes in management and replacement or layoffs of project staff, which in turn might induce loss of trust between the partners, ultimately resulting in financial damage. Hence, especially in IT outsourcing projects, such risks must not be neglected and adequate measures of risk management have to be explored, even if these risks are related to rather rarely occurring events in IT outsourcing. For sustainable success, companies must consider and address even long-term risks to avoid possible future financial exposure.

Financial derivatives are commonly used for hedging market risks and a proved remedy outside the Information Systems (IS) discipline. Instruments like futures or options can be bought to neutralize price risk or provide insurance (Hull, 2009, p. 11). They offer a financial payoff in case of particular events on the markets (e.g. a slump in stock price). This payoff can be used to soften the pain of a financial damage that comes along with such events. Hence, the two IT outsourcing partners could consider hedging the respective risk in their project by using financial derivatives and thereby securing their project cash flows. Until now, IS literature provides different ways of using models from the finance discipline (e.g. real options) for *evaluating* IT projects. In this paper, we show ways of actually *using* (meaning buying) financial derivatives in order to hedge the market risk of outsourced IT projects. In analogy to an insurance contract that covers rare but heavy damages, this hedging approach addresses exceptional events in IT outsourcing that might induce enormous financial damage. It could be argued that this approach is only interesting in times of a financial and economic crisis when presumably solid companies may get under pressure. In contrast, in our paper, we use a formal-deductive and design-oriented model to illustrate that financial hedging might be a reasonable

approach especially in times when there is no crisis and volatility is low, thus helping to survive the next crisis.

II.2.2 Research Objectives

Bahli & Rivard (2003) state that IT outsourcing is believed to generate major benefits, as well as it can be "a risky endeavor" (p. 211). Complementary to the thereby existing project-inherent types of risk, i.e. related to the management of the IT outsourcing project, we want to address the types of risk that depend on changes in the economic condition of the involved outsourcing project partners and are driven first of all by the markets. In this context, the risk of insolvency of the outsourcing project partner is rather uncared for by IS literature up to now and mainly addressed by legal literature, e.g. Spiotto & Spiotto (2003). As possible results of a heavy slump in prices of the client's stocks, IT outsourcing projects may be put on hold or even cancelled, existing budgets may be reduced, and eventual rising loss of trust will lead to a poor outsourcing performance, because trust between the project partners is essential for outsourcing success (Fitzgerald & Willcocks, 1994, p. 94; Han, J. N. Lee, & Seo, 2008, p. 35; Koh, Ang, & Straub, 2004, p. 372; J. N. Lee, 2001. p. 332).

Focusing especially on market impacts that endanger the successful outcome of IT outsourcing projects, our research questions can therefore be posed:

> *How can the risks (a) insolvency of the project partner and (b) a heavy slump in the project partner's stock price be addressed and successfully hedged with the use of financial derivatives?*
>
> *Furthermore, when is a financial hedging approach applicable and when should other means of coverage be used?*

To address these questions, we look at the following dependencies: From the client's point of view, hedging should generate a payoff for the client, if the service provider becomes insolvent. This insolvency is most likely linked to the service provider's stock becoming a penny stock. The payoff should be able to cover the client's financial damage, including e.g. switching costs and lost profit. From the service provider's point of view, hedging should generate a payoff for the service provider, if there is a slump in the client's stock prices. This payoff should be able to cover the service provider's financial damage due to budget cuts, project cancellations, or loss of trust between the two partners.

The client and the service provider might therefore use financial derivatives that pay off if the counterpart's stocks drop under specified thresholds. To cover against the risk of insolvency the client could e.g. buy a derivative that pays off if the service provider's stocks drop below 1$. This will most certainly happen if the service provider files for bankruptcy. The service provider could use a derivative that pays off if the client's stock loses e.g. 30% of its original value, as such a loss might eventually induce financial damage for the service provider.

The paper proceeds as follows: Subsequent to a brief review of the related literature, we present the basic setting and assumptions of our approach. After defining the possible cash flows and their respective probabilities, we develop our objective function. We then analytically identify the optimal degree of hedging. For a deeper analysis, we give a more detailed view on how to calculate the relevant probabilities. A concluding sensitivity analysis provides meaningful and in parts counter-intuitive insights. Finally, we address practical implications and limitations and provide an outlook on possible future research.

II.2.3 Relevant Literature in the Context of Market Risks in IT Outsourcing

IT outsourcing is defined as the decision on relocating IT departments' tasks to a third party vendor (Loh & Venkatraman, 1992, p. 9; Apte et al., 1997, p. 289). The main motives for outsourcing are cost reduction and the focus on core competencies (Dibbern, Goles, Hirschheim, & Jayatilaka, 2004, p. 7; Lacity & Willcocks, 1998, p. 364). Dibbern et al. (2004) and Lacity, Khan, & Willcocks (2009) provide detailed reviews of the IT outsourcing literature. Growing significance and size of IT outsourcing projects lead to an increased concern with the issue of risk mitigation (Willcocks, Lacity, & Kern, 1999, p. 286). Thus, many articles focus on the assessment and controlling of IT outsourcing risk, for example Aron, Clemons, & Reddi (2005), Aubert, Dussault, Patry, & Rivard (1999), Aundhe & Mathew (2009), Fridgen & Müller (2011), Iacovou & Nakatsu (2008), and Taylor (2006).

Very little research exists on dealing with IT outsourcing risks that are not dependent on project management quality but on the economic condition (market risks) of the involved project partners, although these market risks can have heavy negative financial impact, too. Nevertheless, the general importance of these risks (insolvency of the project partner and a heavy slump in prices of the project partner's stocks) has been addressed in IS literature. Regarding the risk of insolvency, Aubert, Patry, & Rivard (2001, p. 6) and Ngwenyama & Sullivan (2006, p. 8) point out that financial stability is an important risk factor in IT outsourcing projects. Kern, Willcocks, & Lacity (2002, p. 118) name the risk of a supplier going

out of business when it comes to outsourcing provider selection. They therefore propose to select a supplier with sound financial position, stable customers, and stable strategic partners as outsourcing partner. Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi (2011, p. 182) name the risk of a service provider's bankruptcy as a legitimate concern when sourcing the IT into the cloud. Though not leading to insolvency, a heavy slump in prices of the counterpart's stocks might have several impacts on an IT outsourcing relationship. While budget cuts and project cancellation by the client are usually not made public, they directly induce financial damage for the service provider. A change of the client's management might furthermore negatively affect the mutual trust between the project partners. Hartman & Ashrafi (2002) empirically confirmed the importance of effective communication on IT projects. Formal outsourcing contracts are important, but trust between the partners is critical for overall outsourcing success (Sabherwal, 1999, p. 85; J. N. Lee, Huynh, & Hirschheim, 2008, p. 147). By using trust-based integrative models and survey data collected from IT outsourcing projects, the importance of trust between service receiver and provider for IT outsourcing success was verified (J. N. Lee et al., 2008; J. N. Lee & Choi, 2011). Fernandez (2003, p. 251) hints on the negative relation between trust and costs of control/safeguard strategies in IT projects. As a conclusion, loss of trust has a negative effect on IT outsourcing success as it leads to increasing costs. Hence, an indirect link between a heavy slump in prices and financial damage due to loss of trust might be conceivable.

In IT outsourcing relationships, service level agreements are a common tool to "monitor the service provider's performance so deficiencies can be adequately measured and penalized" (Goo, Kishore, Rao, & Nam, 2009, p. 140). However, the service provider "can simply go bankrupt and damages may never be recovered" (M. K. O. Lee, 1996, p. 12). The concept of source code escrow should provide access to the source code for the client in the event of the service provider's bankruptcy. Hence, in IT outsourcing projects with focus on software development, a client might use a source code escrow agency to reduce the financial damage in case of an insolvency of the service provider. However, there are many legal difficulties under bankruptcy law and software escrow sometimes fails its essential purpose (Pappous, 1985, p. 326).

The idea of adapting financial methods on IT project management has already been implemented in IS literature. Gull (2011) suggests the usage of options for the valuation of discount options in software license agreements. In addition, existing real options approaches present a theoretical method for evaluating IT projects, but they are no actually purchasable financial derivative. For example, Benaroch (2002) proposes the planning and embedding of

real options in IT investments in order to control various risks. "Options thinking" (p. 75) therefore is a way to acknowledge and manage uncertainty in IT projects (Fichman, Keil, & Tiwana, 2005). However, an approach for hedging financial risks in IT outsourcing projects by actually buying financial derivatives has not been provided yet. We will present such an approach as a first step in such a direction in the following chapter.

II.2.4 A Model Supporting Hedging Decisions in IT Outsourcing

In this chapter, we build an analytical model on how IT outsourcing partners could hedge the risk of insolvency and the risk of a heavy slump in prices by using financial derivatives. We find the optimal hedging strategy and discuss implications.

II.2.4.1 Setting and Assumptions

For reasons of generality, we do not use the terms "client" and "IT service provider", but rather "hedging project partner" (HPP) and "risky project partner" (RPP). HPP is trying to hedge the risk caused by RPP. HPP is not necessarily always the client and RPP is not necessarily always the IT service provider. Instead, the assignment depends on the situation to be examined. We assume a continuous model in which t_0 denotes the beginning and T the end of an IT outsourcing project between HPP and RPP. $r \geq 0$ is defined as the continuous risk-free interest rate.

II.2.4.1.1. Damage, Payoff, and Hedging Instruments

We call the events "damage occurs" $DAMAGE$ and "damage does not occur" $\overline{DAMAGE}$. $DAMAGE$ is caused by RPP and results in negative cash flows in the amount of $\widehat{D} > 0$ for HPP's project. $\overline{DAMAGE}$ has no effect on the project. Our model focuses only on the additional cash flows that are generated by $DAMAGE$ and the hedging decision made by HPP. All other cash flows are supposed certain and are therefore omitted in our model. To decrease model complexity, we apply the following simplifying assumptions that have no major effect on the conclusions that will be drawn later on.

Assumption 1: $DAMAGE$ can only occur in t_{DAMAGE}, with $t_0 < t_{DAMAGE} < T$. t_{DAMAGE} and $\widehat{D}$ are previously known. We assume all model-parameters to be constant over the considered project time.

The limitation of the possible damage to one previously known point in time is a strong assumption and does not picture reality. However, there are financial derivatives that can be

used for hedging a damage that occurs any time. Our model could be adapted accordingly but this would only increase complexity with minimal benefits for our results. For reasons of simplicity, assumption 1 moreover eliminates the possibility that new information is gathered after the IT outsourcing project has started. This reflects the ex-ante planning of an appropriate hedging strategy, which we propose in this paper as a first step in such a direction. Reacting to new information and therefore actively managing the financial hedging portfolio might be a very complex endeavor and is beyond the scope of this paper.

The probability $P(DAMAGE)$ in t_{DAMAGE} is defined as p, with $0 < p < 1$. We can exclude the boundaries 0 and 1 from the domain of p. For $p = 1$, HPP would not accept the project or at least factor the damage $\widehat{D}$ into the contracted price. $p = 0$ is omitted, because there is always a chance for any company to become insolvent or for a heavy slump in prices of its stocks, even if the probability is very small. Earlier, we have discussed special characteristics of an adequate financial derivative, which we refer to as "hedging instrument" from now on. Assumption 2 further defines the hedging instrument.

Assumption 2: The financial market offers a hedging instrument that can generate a payoff in the amount of $\widehat{D}$ in t_{PAYOFF}. We assume $t_{PAYOFF} = t_{DAMAGE} = t$. The hedging instrument is perfectly divisible and there are no transaction costs or taxes.

Assuming the availability of the required derivatives is quite common in the finance discipline, as they can either be created through financial engineering or they will be offered on the market if a demand exists. In practice, options or credit default swaps might be suitable hedging instruments.

An option in general gives the buyer the right, but not the obligation, to buy (call option) or sell (put option) the underlying for a predetermined price to the seller of the option. (Hull, 2009, p. 6) The underlying can be a stock of a particular company, an index, commodities, or currencies, for example. In particularly, a cash-or-nothing put might be a fitting hedging instrument for our purpose. A cash-or-nothing put is a so-called binary option, as it provides a discontinuous payoff. At maturity, it either pays a fixed amount of cash if the underlying ends up below the specified price (strike price), or nothing if it ends up above the specified price (Hull, 2009, p. 553). The stock price of the risky company thereby represents the underlying for the binary option. We are aware that there exists no liquid market for binary options for every company. Nevertheless, there are ways of approximating binary options using more common instruments.

A credit default swap is a derivative that provides insurance explicitly in the case of a default of a particular company. Its basic functional principle is that the buyer of a credit default swap has to pay a (periodic) fee to the seller. In case of a default of the designated company, the seller has to pay a much higher compensatory payment to the buyer. In contrast to an option, here, the underlying is the default of the designated company itself, which is called credit event of the reference entity. (Hull, 2009, p. 518)

We do not limit our approach to these special kinds of financial derivatives. However, we require that the hedging instrument provides a binary payoff depending on the considered risky company's stock price or solvency as an underlying to ensure that the risk can be hedged. Hence, commodities, interest rates, or currencies don't work as an underlying for our approach.

We label the event "hedging instrument pays off" as $PAYOFF$, the event "hedging instrument does not pay off" as $\overline{PAYOFF}$. The probability $P(PAYOFF)$ is defined as q, with $0 < q < 1$. Again, the boundaries 0 and 1 are excluded from the domain of q. For $q = 1$, the price of the hedging instrument equals the present value of its payoff, leaving no opportunity for a hedging strategy. $q = 0$ is omitted because no one would acquire an instrument that never pays off. In many cases, it should be possible to derive the market's opinion on the probability q from the market price of the hedging instrument.

In contrast to an insurance contract, the two events $PAYOFF$ and $DAMAGE$ will not always occur together: It is possible that HPP can get a payoff from the hedging transactions without RPP ever having caused financial damage. (e.g. when a slump in prices doesn't result in budget cuts or loss of trust) On the other hand, HPP could suffer financial damage but not get a payoff from the hedging instrument (e.g. the project is cancelled due to other reasons than the stock price). This leads to four possible situations as presented in table Tab. II-3.

	hedging instrument does not pay off ($\overline{PAYOFF}$)	hedging instrument pays off ($PAYOFF$)
damage does not occur ($\overline{DAMAGE}$)	"regular case" (r)	"best case" (b)
damage occurs ($DAMAGE$)	"worst case" (w)	"hedging case" (h)

Tab. II-3 Overview of Possible Combinations of Events

II.2.4.1.2. Resulting Cash Flows, Decision Situation, and Decision Maker

To identify the optimal degree of hedging, we define the decision variable λ, with $0 \leq \lambda \leq 1$, as the percentage of $\widehat{D}$ to be hedged. $\lambda = 1$ represents hedging the complete amount of damage and $\lambda = 0$ not buying any coverage. For every case, different cash flows may or may not accrue. Figure Abb. II-3 gives a short illustration of the possible cash flows.

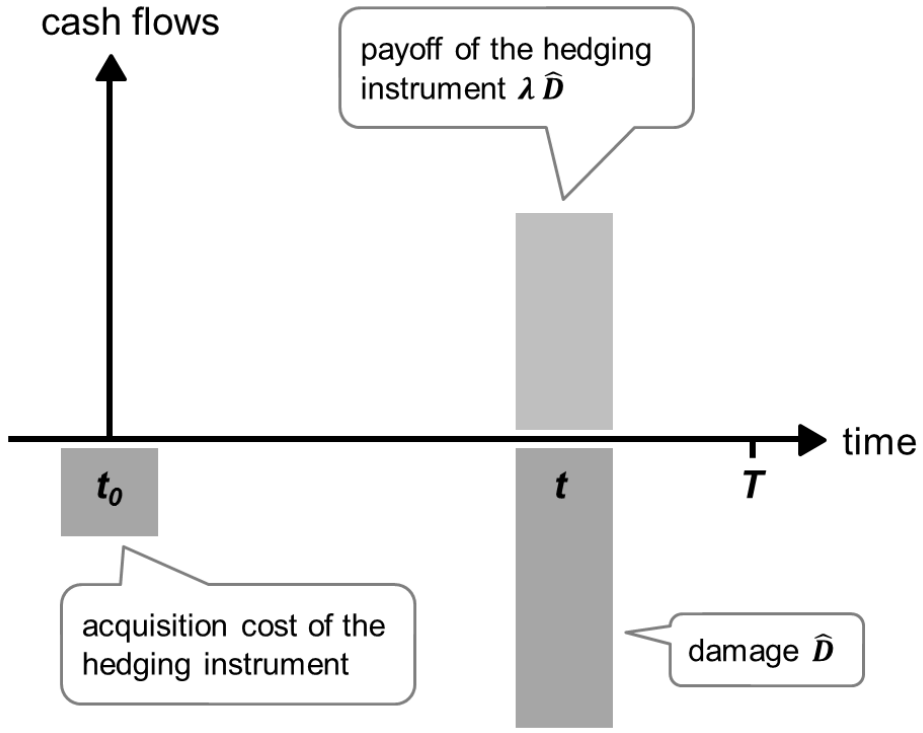

Abb. II-3 Overview of Cash Flows

In t_0, HPP buys the fraction λ of the adequate hedging instrument, which equals hedging a part of the complete possible damage. As the costs for hedging the complete possible damage might be very high, such a practice is quite common for financial hedging attempts. This is possible as we have assumed the hedging instrument to be perfectly divisible. As the hedging instrument provides insurance in case of a default, a price is charged for its acquisition. Following Black & Scholes (1973, p. 644), this price is the discounted expected value of its payoff, considering the likelihood of the event as well as the payoff that might accrue. The acquisition costs are therefore calculated as $\lambda \cdot \widehat{D} \cdot q \cdot e^{-r \cdot t}$ ($e^{-r \cdot t}$ is the general discount factor for the cash flows occurring in t). Similar to an insurance premium, this price has always to be paid, regardless if there will be any default. Therefore, this cash flow accrues with certainty and is not affected by

the ex ante uncertain project situation in t. In t, the possible cash flows depend on the probabilities p and q. $DAMAGE$ occurs with probability p and creates negative cash flows in the amount $\widehat{D}$. As they have to be discounted to t_0, damage is defined as $\widehat{D} \cdot e^{-r \cdot t}$. On the other hand, $PAYOFF$ occurs with probability q and pays off exactly the amount of cash which HPP decided to hedge by choosing λ. The payoff is therefore $\lambda \cdot \widehat{D} \cdot e^{-r \cdot t}$ in t_0. To keep our mathematical approach clear and to save space, we define $D = \widehat{D} \cdot e^{-r \cdot t}$. Table Tab. II-4 provides an overview of the possible cases and the corresponding cash flows that accrue for HPP, with "+" denoting a positive cash flow and "−" denoting a negative cash flow.

	acquisition costs of hedging instrument	damage	payoff of hedging instrument
	$-\lambda \cdot D \cdot q$	$-D$	$+\lambda \cdot D$
regular case	✓		
hedging case	✓	✓	✓
best case	✓		✓
worst case	✓	✓	

Tab. II-4 Overview of Possible Cases and Corresponding Cash Flows

With four possible outcomes, we have to make a choice under uncertainty regarding λ. The optimal degree of hedging λ^* is subject to the individual preferences of the decision maker HPP.

Assumption 3: The decision maker is assumed to be risk-averse and measures utility by $U(x) = -e^{-\alpha \cdot x}$. The decision on the optimal degree of hedging λ^* is made considering the certainty equivalent.

This utility function is compatible to the Bernoulli principle (Bernoulli, 1954). The parameter $\alpha > 0$ is its Arrow-Pratt characterization of absolute risk aversion (Arrow, 1971). The higher the value of α, the more risk-averse HPP. A risk-averse decision maker favors the utility of a risk-free present value over a risky present value with identical expected value. Approaches

similar to our model have been applied numerous times, for example in Freund (1956), Fridgen & Müller (2009), Hanink (1985), Zimmermann (2008), and Zimmermann, Katzmarzik, & Kundisch (2008). Please note that in our case, the utility function $U(x) = -e^{-\alpha \cdot x}$ measures positive and negative cash flows. The presence of risk aversion when valuating negative cash flows is controversially discussed in decision theory literature. We assume risk aversion for positive and negative cash flows, especially under the possible presence of budget restrictions for the project. We use the certainty equivalent principle as a valuation criterion for the best possible hedging implementation, as it is an established method of decision theory (Markowitz, 1959). The equation defining the certainty equivalent has the structure $CE = U^{-1}\left[E\left(U(x)\right)\right]$ and represents the amount of certain payoff which yields the same utility as a risky gamble. In our case, the risky gamble corresponds to hedging the IT outsourcing project which has four possible and therefore risky outcomes (the regular case, the hedging case, the best case and the worst case). To determine the amount of certain payoff, we need the inverse function of the utility function $U^{-1}(x) = -\frac{1}{\alpha} \cdot ln(-x)$. x denotes the utility of the risky gamble, which is the expected utility of its possible outcomes (von Neumann & Morgenstern, 1947).

II.2.4.2 Finding the Optimal Hedging Strategy

To ensure that HPP receives the highest possible utility from the hedging decision according to the given risk aversion α and utility function $U(x)$, we first set up and subsequently maximize the certainty equivalent for λ. Conducting the outsourcing project and applying a hedging strategy that covers the sought degree λ^* of $\widehat{D}$ is therefore the optimal strategy for HPP. Therefore, we consider the utility of the corresponding cash flows for each case. We define the probabilities p_r, p_h, p_b, and p_w as the probabilities of the regular case, the hedging case, the best case, and the worst case, respectively. With the use of Table Tab. II-4 and these probabilities, we can define the certainty CE equivalent for HPP

$$CE = U^{-1}\begin{pmatrix} p_r \cdot U(-\lambda \cdot D \cdot q) + \\ p_h \cdot U(-\lambda \cdot D \cdot q - D + \lambda \cdot D) + \\ p_b \cdot U(-\lambda \cdot D \cdot q + \lambda \cdot D) + \\ p_w \cdot U(-\lambda \cdot D \cdot q - D) \end{pmatrix}$$

The value of CE depends on the degree of hedging λ and indicates the certain amount of money that the hedging decision is worth for HPP. By altering λ, the value of CE also changes. To find the optimal degree λ and therefore the highest possible (or the least negative) value of CE, we differentiate CE for λ. We can show that the calculated candidate for optimality always

represents the optimal degree of hedging λ^* within our model. (see the appendix for equation 1 - 3).

To determine the probabilities p_r, p_h, p_b, and p_w, two additional parameters are introduced that describe the interdependency between $DAMAGE$ and $PAYOFF$: d_1 defines the conditional probability that the hedging instrument creates a payoff if damage is present $P(PAYOFF|DAMAGE)$, with $q < d_1 \leq 1$. d_1 has to be greater than q. This means that $PAYOFF$ is more likely if $DAMAGE$ has occurred. $d_1 = 1$ stands for certain $PAYOFF$ if $DAMAGE$ has occurred. d_2 defines the conditional probability that damage occurs if the hedging instrument creates a payoff $P(DAMAGE|PAYOFF)$, with $p < d_2 \leq 1$. d_2 has to be greater than p. This means that $DAMAGE$ is more likely if the financial market has triggered $PAYOFF$. $d_2 = 1$ stands for certain $DAMAGE$ when $PAYOFF$ exists. These characteristics (increased probability of one event if the other event is also present) should be satisfied by the hedging instrument that HPP selects to ensure its useful adaption. Bayes' theorem requires $d_1 = \frac{q \cdot d_2}{p}$ (Berger, 1985, p. 129). Hence, there is a dependency between the (conditional) probabilities p, q, d_1, and d_2 and only three out of four parameters have to be known. With the use of basic probability theory we can now express p_r, p_h, p_b, and p_w by p, q, d_1, and d_2 (see Table Tab. II-5).

$\overline{DAMAGE} \cap \overline{PAYOFF}$	$DAMAGE \cap PAYOFF$	$\overline{DAMAGE} \cap PAYOFF$	$DAMAGE \cap \overline{PAYOFF}$
p_r	p_h	p_b	p_w
$1 - q - p \cdot (1 - d_1)$	$p \cdot d_1$	$q - p \cdot d_1$	$p \cdot (1 - d_1)$

Tab. II-5 Overview of Probabilities

Please note that d_2 does not appear in any of the cases. This is due to Bayes' theorem, which allows us to replace one of the four probabilities. Using the new probabilities p, q, and d_1, λ^* can be written as

$$\lambda^* = -\frac{1}{\alpha \cdot D} \cdot ln\left(\frac{q}{1-q} \cdot \left(\frac{1 - p \cdot \left(1 + U(-D)\right)}{q - p \cdot d_1 \cdot \left(1 + U(-D)\right)} - 1\right)\right)$$

We are able to find that λ^* is limited to the range $0 < \lambda^* \leq 1$. We can show $\lambda^* > 0$ analytically and confirm $\lambda^* \leq 1$ using a Monte-Carlo simulation. Hence, if we have a suitable hedging instrument, hedging is always superior to non-hedging ($\lambda^* > 0$). The economic interpretation for the upper boundary of λ^* is: Hedging more than the possible damage would induce additional risk with only the expected value in return. As the expected value equals the price of hedging, this will be avoided by the risk-averse decision maker HPP. Thus, the degree of hedging will not exceed 1.

II.2.4.3 Short Example of a Hedging Approach

A client (HPP) initiates a project to source its customer data to the cloud. The storage and support for the data is provided by a big service provider (RPP), which is listed at the stock exchange. To cover a possible damage in case of the default of the service provider, which is assumed to result in $ 10 million damage and might occur in one year, the client considers financial hedging. We assume that the financial market offers a cash-or-nothing put that pays $ 10,000, if the stock of the service provider drops below $ 1.That means, to cover the whole possible damage, the client would need to buy 1,000 contracts of the financial instrument. The financial market estimates the probability for a drop below $ 1 to be 2%. Therefore, the financial instrument is offered for a price of $ 196.04 (risk-free interest rate = 2%). For the case of damage when the customer data is unavailable, we assume the conditional probability to be 90% that the hedging instrument actually pays off. This means that the stocks of the service provider drop below $ 1 at the same time. The client now has to decide how many contracts he wants to buy, from 0 to 1000 contracts for hedging from 0 to 100% of the possible damage. Without hedging, this money could be saved while being exposed to the risk of the full possible damage. Following our optimization, the resulting optimal degree of hedging in this case is $\lambda^* = 61.8\%$, which means that the client should by 618 contracts of the hedging instrument. This provides a 36.3% improvement over the non-hedging alternative (buying 0 contracts). ($p = q = 0.02$, $d_1 = d_2 = 0.9$, $\alpha = 1$, $\widehat{D} = 10$ M., $r = 0.02$, $t = 1$)

II.2.4.4 Sensitivity Analysis

In this chapter, we examine the influences of the individual probabilities on the optimal solution. Therefore we differentiate λ^* in subject to the probabilities and analyze the resulting effects. We have to bear in mind that Bayes' theorem will avoid arbitrarily altering all four parameters at the same time. Therefore we maintain the dependencies between p, q, d_1, and d_2. To study the effect of altered p and q, we assume a fixed interdependency between $DAMAGE$ and $PAYOFF$. Consequently, d_1 and d_2 are treated as constants for the following derivatives. This can be interpreted as sticking to the chosen hedging instrument, which is acquired by the decision maker in t_0. However, with the assumption of fixed conditional probabilities, a variation of p must have an effect on q and vice versa. These effects can be deduced from Bayes' theorem. Hence, the according relation is $q = \frac{d_1}{d_2} \cdot p$ and $p = \frac{d_2}{d_1} \cdot q$, respectively. This means that the probability of payoff that exists at the financial market follows the rising or falling probability of damage. The exact shape of this connection is dependent on the characteristics of the hedging instrument, represented by d_1 and d_2.

To determine the influence of p on λ^* and the influence of q on λ^*, we derive $\frac{\partial \lambda^*}{\partial p}$ and $\frac{\partial \lambda^*}{\partial q}$, respectively (see the appendix for equation 4 - 5). We find $\frac{\partial \lambda^*}{\partial p} < 0$ and $\frac{\partial \lambda^*}{\partial q} < 0$, suggesting a negative relationship. In other words, the higher the probability for $DAMAGE$ or $PAYOFF$, the less hedging is reasonable: The hedging instrument is too expensive compared to its risk reduction. The lower the probability for these two events, the higher the resulting optimal hedging degree: The hedging instrument is cheap enough that its price is overcompensated by the risk reduction. Hence, our hedging approach is not only valid in times of high volatility and therefore high likelihood of damage like in a financial and economic crisis, but proposes cheap hedging in times where probabilities of damage are rather low. In numbers, a rising probability of damage of the service provider in our example from 2% to 20% decreases the optimal hedging degree from 61.8% to 36.5%. On the other hand, a decreasing probability of damage of the service provider from 2% to 0.2% increases the optimal hedging degree from 61.8% to 83.3%.

To study the effect of altered d_1 and d_2, we assume fixed probabilities p and q and derive $\frac{\partial \lambda^*}{\partial d_1}$ and $\frac{\partial \lambda^*}{\partial d_2}$, respectively (see the appendix for equation 6 - 7). We find $\frac{\partial \lambda^*}{\partial d_1} > 0$ and $\frac{\partial \lambda^*}{\partial d_2} > 0$, suggesting a positive relationship. Thus, the greater the interdependency between the two

events, or, in other words, the better fitting the chosen hedging instrument for the according risk, the higher the degree of hedging λ^* that should be chosen. However, the less distinctive the interdependency, the less hedging should be implemented in the outsourcing project. Again in numbers, a rising interdependency between the events of damage and payoff from 90% to 99% increases the optimal hedging degree from 61.8% to 84.1%. On the other hand, a decreasing interdependency from 90% to 50% decreases the optimal hedging degree from 61.8% to 39.7%. This mathematical result can also be explained from an economic point of view: A hedging instrument whose payoff highly echoes the damage of the underlying – in our case the IT outsourcing project – eliminates more "risk-per-dollar" than a hedging instrument that poorly reflects the underlying.

II.2.5 Practical Implications, Limitations and Outlook

This paper focuses on market risks in IT outsourcing projects that today are only addressed in a qualitative way in outsourcing literature, but that have not been quantitatively approached up to now. Their relevance has been fortified in the latest financial and economic crisis and they should therefore be adequately treated by IT decision makers. As a first step, we propose an innovative hedging approach based on financial derivatives to address these risks with the use of a quantitative decision model. The findings are as follows:

> *Result 1*: Firms should always consider financial hedging for the addressed types of IT outsourcing risk if a fitting financial derivative is available.
>
> *Result 2*: The more likely your project partner will cause damage, e.g. in times of a financial and economic crisis, the more expensive are hedging instruments on the financial markets and the less money should be spent for financial hedging. In contrast, you should buy more cheap financial derivatives for hedging, especially when no crisis is present and the probability of damage is very low.
>
> *Result 3:* The better your hedging instrument fits, meaning the more "risk-reduction-per-dollar" it provides, the more hedging should be applied.

As the optimal degree of hedging determined by the model is continuous, there is no explicit line dividing a low risk from a high risk, nor one dividing a cheap hedging instrument from an expensive hedging instrument. However, the model in this paper can determine the optimal degree of hedging for any given risk and therefore gives a hint on how much you should rely on financial hedging compared to other strategies. When risk is high and hedging on the

financial market is very expensive, other means of risk mitigation should be considered. As service level agreements are useless when the contractual partner defaults, software escrow might be a minor remedy, despite its before mentioned weaknesses. In addition, literature suggests the concept of multi-sourcing, which might be a solution to some extent, especially in cloud computing sourcing settings, e.g. as described in König et al. (2013). Moreover, a financially stable project partner might consider buying its counterpart to ensure the survival of the latter one, thus turning an outsourcing setting into an in-house production. Such backward integration might be reasonable if the client buys the service provider, but not vice versa. In every case, one should question the financial stability of the project partner before the start of the IT outsourcing project. If a rather high risk of default is detected, conducting the project with an entire different project partner should be considered instead of hedging.

The restricting assumptions of this paper are necessary to maintain a comprehensible analytical approach. In the following, we address these restrictions. In assumption 1, the limitation of the possible damage to one ex ante known point in time does not necessarily picture reality. This could be addressed in the model by introducing distributions for probability and amount of damage with respect to time. In assumption 2, we claimed the financial derivative to pay off when damage occurs. This does not represent a problem as long as the only time of possible damage is previously known. Without assumption 1, the financial derivative must be able to pay off at every time damage can occur. The increased flexibility of such a financial derivative leads to higher hedging costs and therefore intensifies the negative relation between probability of default and degree of hedging. Giving up the neglected transaction costs and taxes has the same effect. A general difficulty is the determination of the required probabilities. While the probability of payoff should be easy to obtain at the financial markets and might hint on the appropriate value for the probability of damage, the conditional probabilities might be more of a problem and remain subject to the estimation of the decision maker. Nevertheless, there seems to be no reason why the effects we have discovered should fundamentally change when relaxing our assumptions.

Besides these restrictions, there is of course a lot of potential for further research. First, the client might not solely want to hedge the insolvency of the service provider but also try to cover financial damage due to a slump in prices of the service provider (which might occur in different intensities for different triggers). Here, it might be reasonable to hedge many different triggers with many financial derivatives. Hence, the examination of the optimal hedging strategy in such cases may be a next step. Second, it would be interesting to consider that client has several

ongoing IT outsourcing projects with different IT service providers. The resulting individual hedging instruments may correlate with each other, making it necessary to examine the entire IT outsourcing project portfolio as a whole (Lacity & Willcocks, 2003, p. 116), including hedging instruments. This extension could integrate hedging into existing IT sourcing portfolio management theory as proposed by Verhoef (2005), Wehrmann, Heinrich, & Seifert (2006), and Zimmermann et al. (2008). Third, there is potential for risk adjusted pricing approaches for IT outsourcing services. A financial stable service provider could anticipate that its project partners have a cheap hedging possibility resulting from its low probability of damage. Therefore, it might be able to charge more for its services than a smaller service provider with a higher probability to create damage and thus higher hedging costs for the client.

Although in practice our model is most likely not suitable to exactly determine an optimal degree of hedging which can directly be implemented in IT outsourcing projects, a reasonable estimation is still better than completely ignoring the risk. Our model provides a theoretically sound economical approach that should encourage companies to start thinking about using financial instruments to hedge existing market risks in their IT outsourcing projects. In the future, we have to extend our view on further opportunities to adapt this idea on other types of IT project risk.

II.2.6 References

Apte, U. M., Sobol, M. G., Hanaoka, S., Shimada, T., Saarinen, T., Salmela, T., & Vepsalainen, A. P. J. (1997). IS Outsourcing Practices in the USA, Japan and Finland: A Comparative Study. *Journal of Information Technology*, 12(4), 289-304.

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just Right Outsourcing: Understanding and Managing Risk. *Journal of Management Information Systems*, 22(2), 37-55.

Arrow, K. J. (1971). The Theory of Risk Aversion. In K. J. Arrow (Ed.), *Essays in the Theory of Risk-Bearing* (1st ed., pp. 90-120). Chicago: Markham.

Aubert, B. A., Dussault, S., Patry, M., & Rivard, S. (1999). Managing the Risk of IT Outsourcing. *Proceedings of the 32nd Hawaii International Conference on System Science*, Los Alamitos.

Aubert, B. A., Patry, M., & Rivard, S. (2001). Managing IT Outsourcing Risk: Lessons Learned. *CIRANO Working Papers* 2001s-39.

Aundhe, M. D., & Mathew, S. K. (2009). Risks in offshore IT outsourcing: A service provider perspective. *European Management Journal*, 27(6), 418-428.

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology*, 18(3), 211-221.

Baker, S., Spiro, M. & Hamm, S. (2000). The Fall of Baan (int'l edition). Retrieved from http://www.businessweek.com/2000/00_33/b3694015.htm

Benaroch, M. (2002). Managing Information Technology Investment Risk: A Real Options Perspective. *Journal of Management Information Systems*, 19(2), 43-84.

Berger, J. O. (1985). *Statistical Decision Theory and Bayesian Analysis*. New York: Springer.

Bernoulli, D. (1954). Exposition of a New Theory on the Measurement of Risk. *Econometrica*, 22(1), 23-36.

Black, F., & Scholes, M. (1973). The Pricing of Options and Corporate Liabilities. *Journal of Political Economy*, 81(3), 637-654.

Business Wire India (2007). Wipro and Nortel win Outsourcing Excellence Award. Retrieved from http://www.businesswireindia.com/pressrelease.asp?b2mid=13506

CBC News (2009). Nortel Networks files for bankruptcy protection. Retrieved from http://www.cbc.ca/news/business/story/2009/01/14/nortelbankruptcypro.html

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information Systems Outsourcing: A Survey and Analysis of the Literature. *ACM SIGMIS Database*, 35(4), 6-102.

Feeny, D. F., & Willcocks, L. P. (1998). Core IS capabilities for exploiting information technology. *Sloan Management Review*, 39(3), 9-21.

Fernandez, W. D. (2003). Metateams in Major Information Technology Projects: A Grounded Theory on Conflict, Trust, Communication, and Cost. University of Technology, Queensland.

Fichman, R. G., Keil, M., & Tiwana, A. (2005). Beyond Valuation: Options Thinking in IT Project Management. *California Management Review*, 47(2), 74-96.

Fitzgerald, G., & Willcocks, L. (1994). Contracts and Partnerships in the Outsourcing of IT. *Proceedings of the 15th International Conference on Information Systems*, Washington.

Freund, R. J. (1956). The Introduction of Risk into a Programming Model. *Econometrica*, 24(3), 253-263.

Fridgen, G., & Müller, H. V. (2009). Risk/Cost Valuation of Fixed Price IT Outsourcing in a Portfolio Context. *Proceedings of the 30th International Conference on Information Systems*, Phoenix.

Fridgen, G., & Müller, H. V. (2011). An Approach for Portfolio Selection in Multi-Vendor IT Outsourcing. *Proceedings of the 32nd International Conference on Information Systems*, Shanghai.

Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2009). The Role of Service Level Agreements in Relational Management of IT Outsourcing: An Empirical Study. *MIS Quarterly*, 33(1), 119-145.

Gull, D. (2011). Valuation of Discount Options in Software License Agreements. *Business & Information Systems Engineering*, 3(4), 221-230.

Han, H. S., Lee, J. N., & Seo, Y. W. (2008). Analyzing the impact of a firm's capability on outsourcing success: A process perspective. *Information & Management*, 45(1), 31-42.

Hanink, D. M. (1985). A Mean-Variance Model of MNF Location Strategy. Journal of *International Business Studies*, 16(1), 165-170.

Hartman, F., & Ashrafi, R. A. (2002). Project Management in the Information Systems and Information Technologies Industries. *Project Management Journal*, 33(3), 5-15.

Hull, J. (2009). *Options, Futures, and Other Derivatives* (7.th ed.). New Jersey: Pearson Education.

Iacovou, C. L., & Nakatsu, R. (2008). A Risk Profile of Offshore-Outsourced Development Projects. *Communications of the ACM*, 51(6), 89-94.

Kern, T., Willcocks, L. P., & Lacity, M. C. (2002). Application service provision: Risk assessment and mitigation. *MIS Quarterly Executive*, 1(2), 113-126.

König, C., Mette, P., & Müller, H. V. (2013). Multivendor Portfolio Strategies in Cloud Computing. *Proceedings of the 21th European Conference on Information Systems*, Utrecht.

Koh, C., Ang, S., & Straub, D. W. (2004). IT Outsourcing Success: A Psychological Contract Perspective. *Information Systems Research*, 15(4), 356-373.

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *The Journal of Strategic Information Systems*, 18(3), 130-146.

Lacity, M. C., & Willcocks, L. P. (1998). An Empirical Investigation of Information Technology Sourcing Practices: Lessons from Experience. *MIS Quarterly*, 22(3), 363-408.

Lacity, M. C., & Willcocks, L. P. (2003). IT Sourcing Reflections: Lessons for Customers and Suppliers. *Wirtschaftsinformatik*, 45(2), 115-125.

Lee, J. N. (2001). The impact of knowledge sharing, organizational capability and partnership quality on IS outsourcing success. *Information & Management*, 38(5), 323-335.

Lee, J. N., Huynh, M. Q., & Hirschheim, R. (2008). An integrative model of trust on IT outsourcing: Examining a bilateral perspective. *Information Systems Frontiers*, 10(2), 145-163.

Lee, J. N., & Choi, B. (2011). Effects Of Initial And Ongoing Trust In It Outsourcing: A Bilateral Perspective. *Information & Management*, 48(2-3), 96-105.

Lee, M. K. O. (1996). IT outsourcing contracts: practical issues for management. *Industrial Management & Data Systems*, 96(1), 15-20.

Loh, L., & Venkatraman, N. (1992). Determinants of Information Technology Outsourcing: A Cross-Sectional Analysis. *Journal of Management Information Systems*, 9(1), 7-24.

Markowitz, H. M. (1959). *Portfolio Selection: Efficient Diversification of Investments*. New York: John Wiley & Sons, Inc.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176-189.

Ngwenyama, O. K., & Sullivan, W. E. (2006). Secrets of a Successful Outsourcing Contract: A Risk Analysis. *Proceedings of the 14th European Conference on Information Systems*, Göteborg.

Pappous, P. A. (1985). The Software Escrow: The Court Favorite and Bankruptcy Law. *Santa Clara Computer & High Tech.LJ*, 1, 309.

Sabherwal, R. (1999). The Role of Trust in Outsourced IS Development Projects. *Communications of the ACM*, 42(2), 80-86.

Spiotto, A. H., & Spiotto, J. E. (2003). The Ultimate Downside of Outsourcing: Bankruptcy of the Service Provider. *American Bankruptcy Institute Law Review*, 11(1), 47-92.

Taylor, H. (2006). Critical Risks in Outsourced IT Projects: The Intractable and the Unforeseen. *Communications of the ACM*, 49(11), 75-79.

Verhoef, C. (2005). Quantifying the value of IT-investments. *Science of Computer Programming*, 56(3), 315-342.

von Neumann, J., & Morgenstern, O. (1947). *The Theory of Games and Economic Behaviour*. Princeton: Princeton University Press.

Wehrmann, A., Heinrich, B., & Seifert, F. (2006). Quantitatives IT-Portfoliomanagement: Risiken von IT-Investitionen wertorientiert steuern. *Wirtschaftsinformatik*, 48(4), 234-245.

Willcocks, L. P., Lacity, M. C., & Kern, T. (1999). Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA. *Journal of Strategic Information Systems*, 8(3), 285-314.

Zimmermann, S. (2008). Governance im IT-Portfoliomanagement - Ein Ansatz zur Berücksichtigung von Strategic Alignment bei der Bewertung von IT. *Wirtschaftsinformatik*, 50(5), 357-365.

Zimmermann, S., Katzmarzik, A., & Kundisch, D. (2008). IT Sourcing Portfolio Management for IT Service Providers - A Risk/Cost Perspective. *Proceedings of the 29th International Conference on Information Systems*, Paris.

II.2.7 Appendix

To find the optimal degree λ, which yields the highest possible CE, we differentiate CE for λ:

$$\frac{\partial CE}{\partial \lambda} = -D \cdot q - \frac{1}{\alpha} \cdot \frac{\alpha \cdot D \cdot p_h \cdot U(-D + \lambda \cdot D) + \alpha \cdot D \cdot p_b \cdot U(\lambda \cdot D)}{p_r - p_h \cdot U(-D + \lambda \cdot D) - p_b \cdot U(\lambda \cdot D) - p_w \cdot U(-D)} \tag{1}$$

To fulfill the first order condition for optimality, we set the first derivative equal to 0. By solving $\frac{\partial CE}{\partial \lambda} = 0$ for λ we get a candidate for optimality $\check{\lambda}$:

$$\check{\lambda} = -\frac{1}{\alpha \cdot D} \cdot ln\left(\frac{q \cdot \left(p_r - p_w \cdot U(-D)\right)}{(1-q) \cdot \left(p_b - p_h \cdot U(-D)\right)}\right) \tag{2}$$

To fulfill the second order condition for optimality, the second derivative $\frac{\partial^2 CE}{\partial \lambda^2}$ has to be negative. Hence, we differentiate $\frac{\partial CE}{\partial \lambda}$ for λ:

$$\frac{\partial^2 CE}{\partial \lambda^2} = \frac{\left(\alpha \cdot D^2 \cdot p_h \cdot U(-D + \lambda \cdot D) + \alpha \cdot D^2 \cdot p_b \cdot U(\lambda \cdot D)\right) \cdot \left(p_r - p_w \cdot U(-D)\right)}{\left(p_r - p_h \cdot U(-D + \lambda \cdot D) - p_b \cdot U(\lambda \cdot D) - p_w \cdot U(-D)\right)^2} \tag{3}$$

$\frac{\partial^2 CE}{\partial \lambda^2} < 0$ resolves to $p_b > p_h \cdot U(-D)$, which is always true, considering the probabilities being positive and the utility of a negative value being negative. According to our findings in the sensitivity analysis, $0 < \check{\lambda} \leq 1$. Therefore, $\lambda^* = \check{\lambda}$ represents the optimal degree of hedging within our model setting.

To determine the influence of p on λ^*, we substitute $q = \frac{d_1}{d_2} \cdot p$ and derive $\frac{\partial \lambda^*}{\partial p}$.

$$\frac{\partial \lambda^*}{\partial p} = \frac{{d_2}^2 \cdot (1 - d_1) \cdot \left(1 + U(-D)\right)}{\alpha \cdot D \cdot (d_1 \cdot p - d_2) \cdot \left[d_1 \cdot p + d_2 \cdot p \cdot (1 - d_1) \cdot \left(1 + U(-D)\right) - d_2\right]} \tag{4}$$

In analogy, the influence of q on λ^* is described by the derivative $\frac{\partial \lambda^*}{\partial q}$ with the substitution $p = \frac{d_2}{d_1} \cdot q$.

$$\frac{\partial \lambda^*}{\partial q} = \frac{d_2 \cdot (1 - d_1) \cdot \big(1 + U(-D)\big)}{\alpha \cdot D \cdot (q - 1) \cdot \big[d_1 \cdot (q - 1) + d_2 \cdot q \cdot (1 - d_1) \cdot \big(1 + U(-D)\big)\big]} \tag{5}$$

We find $\frac{\partial \lambda^*}{\partial p} < 0$ and $\frac{\partial \lambda^*}{\partial q} < 0$.

To study the effect of altered d_1 and d_2, we assume fixed probabilities p and q and treat them as constants, when deriving $\frac{\partial \lambda^*}{\partial d_1}$ and $\frac{\partial \lambda^*}{\partial d_2}$.

$$\frac{\partial \lambda^*}{\partial d_1} = \frac{-p \cdot \big(1 + U(-D)\big) \cdot \big[1 - p \cdot \big(1 + U(-D)\big)\big]}{\alpha \cdot D \cdot \big[q - p \cdot d_1 \cdot \big(1 + U(-D)\big)\big] \cdot \big[p \cdot (1 - d_1) \cdot \big(1 + U(-D)\big) + q - 1\big]} \tag{6}$$

$$\frac{\partial \lambda^*}{\partial d_2} = \frac{-\big(1 + U(-D)\big) \cdot \big[1 - p \cdot \big(1 + U(-D)\big)\big]}{\alpha \cdot D \cdot \big[1 - d_2 \cdot \big(1 + U(-D)\big)\big] \cdot [q \cdot (1 - d_2) - (d_2 \cdot q - p) \cdot U(-D) + p - 1]} \tag{7}$$

We find $\frac{\partial \lambda^*}{\partial d_1} > 0$ and $\frac{\partial \lambda^*}{\partial d_2} > 0$.

III Risikoidentifikation und Risikosteuerung in Netzwerkstrukturen

Nachdem in Kapitel II die Aspekte der Risikoidentifikation und Risikosteuerung in bilateralen IT-Sourcing-Beziehungen behandelt wurden, wird nun der Fokus hin zu Netzwerkstrukturen erweitert. Hierzu werden in Kapitel III einerseits IT-Sourcing-Netzwerke aus verschiedenen Cloud-Computing-Akteuren betrachtet, andererseits Netzwerke zum Bezug von Rohstoffen, die sich aus dem Zusammenspiel von Zulieferern, Kunden und weiteren Einflussfaktoren ergeben. Die in Kapitel II identifizierten Risiken und die exemplarisch untersuchte Methode zur Risikosteuerung sind dabei auch für die in Kapitel III untersuchten Netzwerkstrukturen von Relevanz. In Beitrag 3 werden zunächst Taxonomien von Cloud-Computing-Akteuren und von Risiken in Cloud-Computing-Netzwerken entwickelt, welche als Basis für die darauf folgende Entwicklung eines Referenzmodells dienen. Mittels des Referenzmodells lassen sich einerseits Netzwerkstrukturen visualisieren, um die aktuell vorherrschende Intransparenz zu bekämpfen, andererseits aber auch die Weitergabe und Ausbreitung von Risiken in diesen Netzwerken abbilden. Damit unterstützt Beitrag 3 die Risikoidentifikation in IT-Sourcing-Netzwerken. Beitrag 4 untersucht strukturverwandte Netzwerke zum Rohstoffbezug, um dortige Lösungsansätze künftig auch für IT-Sourcing-Netzwerke übertragbar zu machen. Anhand einer entwickelten strukturierten Übersicht können einerseits mögliche Risiken identifiziert und andererseits Absicherungsmaßnahmen zur Steuerung dieser Risiken gefunden werden.

III.1 Beitrag 3: „A Reference Model to Support Risk Identification in Cloud Networks“

Autoren:	Robert Keller, Christian König Kernkompetenzzentrum Finanz- & Informationsmanagement, Lehrstuhl für BWL, Wirtschaftsinformatik, Informations- & Finanzmanagement (Prof. Dr. Hans Ulrich Buhl) Universität Augsburg, D-86135 Augsburg {robert.keller, christian.koenig}@fim-rc.de

Erscheint 2014 in:	Proceedings of 35th International Conference on Information Systems (ICIS), Auckland, New Zealand

Zusammenfassung:

The rising adoption of cloud computing and increasing interconnections among its actors lead to the emergence of network-like structures and new associated risks. A major obstacle for addressing these risks is the lack of transparency concerning the underlying network structure and the dissemination of risks therein. Existing research does not consider the risk perspective in a cloud network's context. We address this research gap with the construction of a reference model that can display such networks and therefore supports risk identification. We evaluate the reference model through real-world examples and interviews with industry experts and demonstrate its applicability. The model provides a better understanding of cloud networks and causalities between related risks. These insights can be used to develop appropriate risk management strategies in cloud networks. The reference model sets a basis for future risk quantification approaches as well as for the design of (IT) tools for risk analysis.

III.1.1 Introduction

Cloud computing has emerged as a new outsourcing paradigm during the last few years (Bresnahan et al. 2011). In 2013, the yearly spending on cloud computing nearly hit the 50 billion dollar mark and is expected to climb up to over 100 billion dollars in 2017 (IDC 2013). Accompanied by rising adoption, the inherent risks of cloud computing must be addressed. Recent IS research examines these risks, for example, see Armbrust et al. (2009), Troshani et al. (2011), or Clarke (2012a). Additionally, risk avoiding strategies like multi-sourcing (AlZain et al. 2012) or attack avoiding strategies (Zissis and Lekkas 2012) are described and may be progressively adopted in practice. Therefore in the future, even more companies will dare to move into the cloud when cloud computing has overcome its current Trough of Disillusionment (Linden and Fenn 2003) with the guidance of IS research.

The increasing adoption of cloud services and rising interconnections among actors in cloud computing lead to the emergence of network-like structures in the cloud business. These structures are similar to complex supply networks known from the manufacturing industries (compare Hallikas et al. 2002). In the following, we will refer to these structures as cloud networks.

Besides “traditional” cloud computing risks that mostly focus on a vendor or a customer, new network-induced kinds of risk are emerging and should be addressed by adequate risk management practices, anchored in IT governance. An incident at one place can lead to cascading effects that affect many other participants in the network. Cloud networks may adopt some characteristics and risks of supply chain networks or even the financial industry (compare Buyya et al. (2008)). In 2011, for example, an outage of Amazon EC2 occurred which affected many of its customers (Clarke 2012b). Among them were Heroku, Engine Yard, and DotCloud, which build their platform services on Amazon’s EC2 infrastructure services and provide them to other companies like ASICS or Audi that were consequently not able to provide their built-on application services to their respective customers (Harris 2011).

One major obstacle for addressing these risks in cloud networks is the lack of knowledge on the underlying network structure and thus, the possible risks. Without this knowledge, no appropriate risk management strategy can be applied. Until now, the existing literature on risks in cloud computing focuses mostly on compliance and general risk management approaches as well as on identification and quantification of risks for a specific company. For example, Martens and Teuteberg (2011) designed a reference model for risk and compliance management

for cloud services. Wherein the authors aim to "support companies in managing and reducing risk and compliance efforts" (Martens and Teuteberg 2011). They provide a UML (OMG 2011) class diagram that describes the required components of cloud risk management in companies. Armbrust et al. (2009) or Dillon et al. (2010) focus on the risk identification from a technological point of view at the customer side. Several authors provide approaches to measure cloud risks. For example, Harnisch and Buxmann (2013) evaluate cloud services with methods of supplier selection and Saripalli and Walters (2010) propose a quantitative impact and risk assessment framework for cloud security. However, we have not found any approaches that examine risks of cloud computing from a network perspective. Authors that do focus on cloud networks, such as Böhm et al. (2010), Marinos and Briscoe (2009), or Bleizeffer et al. (2011), do not consider risks in their approaches.

In this paper, we will answer the following research questions as a first step to address this lack of knowledge:

RQ1: What actors exist in cloud networks?

RQ2: What risks affect the actors of cloud networks?

On this basis, we construct a reference model that contributes to the understanding of the nexus of globally distributed cloud networks and its respective risks. The goal of a reference model is to cover "general patterns in order to raise the efficiency and effectiveness of specific modeling processes" (Vom Brocke and Thomas 2006). In line with Hevner et al. (2004), we build our reference model as a specific "artifact" and evaluate it in the course of our search process, which is similar to the approach of Knackstedt et al. (2009). In order to "enhance the quality" of our reference model, we follow the "guidelines of modeling" by Schuette and Rotthowe (1998). We use a slightly simplified version of UML (OMG 2011) as a semi-formal modeling language for information modeling in order to describe our artifacts in a clear and comprehensible manner. We examine actors and risks of cloud networks and display them in tree based structures through generalizations in UML class diagrams. These two taxonomies (RQ1 and RQ2) build a solid basis for our reference model. The taxonomies are grounded on existing literature in cloud computing and related literature from other disciplines, such as supply chain networks or the financial industry, and then elaborated with our own critical reflection. We develop the reference model by identifying connections between actors and the causalities between different risks, respectively. The taxonomies are evaluated trough real world examinations following a conceptual-to-empirical approach proposed by Nickerson et al.

(2013). In addition, we discussed the taxonomies with industry experts to guarantee the reflection of existing market structures. The reference model is also evaluated in discussions with industry experts. Furthermore, we elaborate the reference model through instantiation on the basis of a real world example to demonstrate its applicability. We used the insights from the interviews to improve the taxonomies and the reference model. Due to the limited space, we only illustrate the final versions of our reference model and the partial models. We describe the iteration steps of improvement in the evaluation section.

On the basis of our reference model, the dissemination of risks throughout the cloud network can be examined. In this context, dissemination describes the passing on of a risk from one actor to another whereby the first actor still is affected. Practitioners can display relevant actors and structures in cloud networks. By using the reference model as a template and instantiating it for their specific scenarios, they can identify impending risks. In addition, the reference models supports a better understanding of the effects of risks on the holistic system. Referring to the risk cycle of Zhang et al. (2010), our reference model enables practitioners to select relevant critical areas and identify the respective occurring risks. The reference model displayed in a semi-formal diagram sets a basis for future risk quantification approaches as well as for the design of (IT) tools for risk analysis. On this basis, appropriate risk management strategies can be developed.

The paper is structured as follows: To address the problem relevance, we outline the development towards cloud networks in Section 2. In Section 3 and 4, we develop a taxonomy of actors in cloud networks and a taxonomy of risks in cloud networks. In Section 5, we create two partial models based on the two taxonomies. Finally, we merge these two partial models to the reference model. In Section 6, we provide an evaluation of the taxonomies and the reference model. In Section 7, we discuss implications, address the applicability of the model and provide an outlook on future research.

III.1.2 Developments towards Cloud Networks

In addition to the increasing adoption of cloud services, we observe new developments in cloud computing. These developments lead to the aforementioned emergence of cloud networks:

- First, a trend towards an increasing *standardization* in cloud computing exists (Vaquero et al. 2009), strengthening the interchangeability of cloud services between different actors in cloud computing. In an outlook on future market structures, Buyya et al. (2008) describe cloud exchanges with brokers that trade standardized cloud products.

- Second, the *specialization* of cloud services increases to provide software for specific "intended user groups" such as private users or specific business groups (Höfer and Karagiannis 2010). Due to low barriers to market entry (Clemons and Chen 2011), a huge variation of application services surfaces.
- Third, the *dependencies* among actors in cloud networks are rising. These dependencies are caused by the aforementioned developments as well as the concept of multi sourcing in the cloud to prevent outages, as suggested by Armbrust et al. (2009) and analyzed by König et al. (2013).

In addition, new market structures and actors emerge in cloud computing. Some companies developed to large players in cloud computing during the last years, such as Amazon, Salesforce, or Microsoft. On the one hand, the variety of offerings on the infrastructure as a service (IaaS) market shrinks as the large players offer lower prices and higher availability than mid-size infrastructure providers could ever achieve (Harris 2014). On the other hand, the variety of software as a service (SaaS) offerings enlarges. This leads to a market with a lack of transparency where many different actors *depend* on only a few. In this market, we observe the genesis of new business models like the Deutsche Boerse Cloud Exchange or the Massachusetts Open Cloud project as an exchange platform for *standardized* infrastructure services, or VMware Service Market Place and the HP Aggregation Platform which offer software and platform services. Actors in cloud computing are now able to outsource *specialized* functions (Troshani et al. 2011). Thereby, they can focus on their core competencies by consuming other *specialized* cloud services in order to simplify their operational business or enhance their own service offerings. Vendors may, for example, use payment handling services and development platform services from other cloud actors to provide their own application services. Market places strengthen the bonding between actors of a cloud network, while facilitating a rapid exchange of cloud services. This development is especially displayed in *standardized* interfaces in cloud market places and in a strong movement towards *standardization*, pushed forward by organizations such as the "Cloud Standards Customer Council" with important industry players like IBM or Symantec (Cloud Standards Customer Council 2014). The emergence of cloud exchange markets will in turn additionally strengthen the drive for *standardization* of cloud services (see Buyya et al. (2008)).

These developments are likely to transform the current cloud landscape towards complex, globally distributed cloud networks, consisting of many different actors and connections. In these cloud networks, risks can disseminate between different actors. For example, Microsoft

Yammer, an enterprise social network that supports collaboration between employees, uses the cloud service Crocodoc to convert PDF and Microsoft Word Documents into HTML5. Crocodoc itself is hosted by Amazon Web Services (AWS). Hence, the services from Microsoft depends to some extent on the availability of AWS. A recently emerged risk occurred after Facebook bought Instagram and released new license agreements. The emerging bad publicity on Instagram pushed many users to services of competitors. These competitors were then struggling to provide the required infrastructure resources in short-term to keep their services running (Laurent 2013).

III.1.3 Taxonomy of Actors in Cloud Networks

Several cloud computing taxonomies exist in IS literature, such as Hoefer and Karagiannis (2010), Hoefer and Karagiannis (2011), or Rimal et al. (2009). These taxonomies classify cloud services in terms of technical properties. In contrast to these approaches, we focus on the business perspective of cloud computing. Within this perspective, we only consider actors that participate in the production of cloud services and therefore provide, process, or transmit services in cloud networks. As a basis for the construction of our taxonomy, we refer to Böhm et al. (2010) who address "the business perspective of IT provisioning", and extend it with results of other authors. Leimeister et al. (2010) describe the value transfer between actors in cloud computing. In addition, we use the differentiation of provisioning models that is described by Marinos and Briscoe (2009). They identify "vendors", "developers", and "end users" as actors related to IaaS, platform as a service (PaaS), and SaaS, which are described in detail in the ontology of Youseff et al. (2008). Marinos and Briscoe (2009) state that a "vendor" provides IaaS, PaaS, and SaaS whereas the "developer" consumes IaaS and PaaS and provides SaaS. The "end user" consumes SaaS. We adopt this "input/output" view for our classification logic.

As mentioned earlier, cloud networks may share some characteristics with supply chain networks and the financial industry. Regarding supply chain literature, such as Lambert et al. (1998) or Harland (1996), we identified equivalents to the actors that are already described in the literature on cloud computing. In a supply chain network, many customer/vendor relationships exist, including value-adding steps between the stages of the production process. Each producer is able to produce goods parallel or sequential to other producers. We adopt the way of distinguishing actors between the respective positions in the network and between the respective products. Regarding the financial industry, the interconnections of banks and other financial institutions with their respective dependencies can be compared to the

interconnections among cloud services to some extent. Information is exchanged in real time and is often organized as an on demand self-service. Certain actors, such as the exchange market or aggregator/broker, already exist or are evolving in cloud computing. From the financial industry we additionally adopt the actor "market place" and the idea of a liquid market where standardized cloud services are exchanged.

Our taxonomy is based on existing literature with a focus on the business perspective and extended with our own observations. Within the taxonomy, we categorize the actors with the help of three layers:

- In a *Position Layer*, we distinguish between the positions of the actors in a cloud network. A *Provider* is the first node in the network whereas the *Client* represents the final node. Between these nodes we identified *Intermediaries* that use services produced by other participants of the cloud network, enhance or aggregate these services, and provide them afterwards to their own customers.
- In a *Business Model Layer*, we distinguish within the three categories of the position layer and consider the different business models of the respective actors. We regard *Initial Producers*, *Value-Added Resellers*, and *Catalysts* which strengthen the interconnections among cloud actors and increase the frequency and easiness of interactions (like market liquidity) in the cloud network.
- A *Product Layer* specifies the actors by the respective provided product. Therefore we use the technical layers of cloud computing (IaaS, PaaS, SaaS). In addition, we introduce the *Aggregator* as a new form of a *Value-Added Reseller*.

In order to address research question *RQ1*, we illustrate the hierarchical taxonomy of actors in a UML class diagram in figure Abb. III-1 through generalizations. A generalization represents an "is a" relationship whereby a specific element "inherits the features of the more general" element (OMG 2011). The taxonomy contains all identified *Actors*, layers, and inheritance between the layers. The classes of the *Position Layer* inherit from the super-class *Actor*. The classes of the *Business Model Layer* inherit from the super-classes in the *Position Layer*. The classes of the *Product Layer* inherit from the super-classes in the *Business Model Layer*. It can be read as follows: An *Aggregator* is a *Value-Added Reseller* is an *Intermediary* is an *Actor*. We explain the identified *Actors* in detail on a *Product Layer* level in table Tab. III-1 in the appendix.

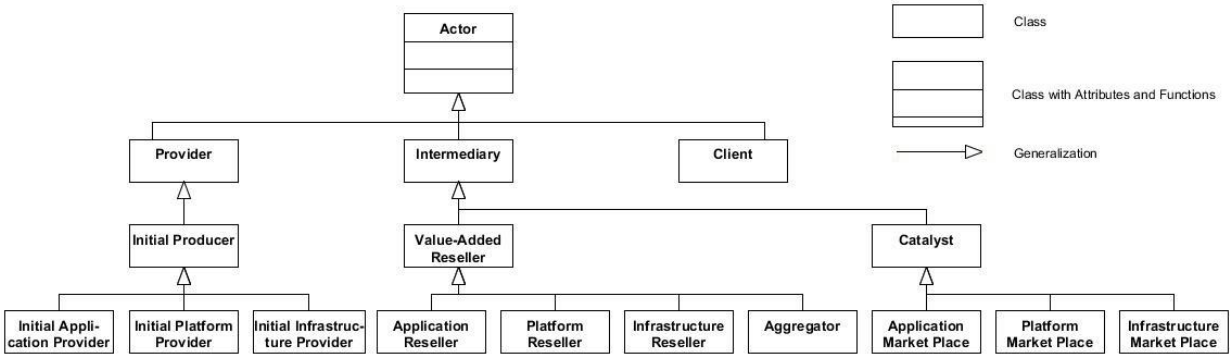

Abb. III-1 Taxonomy of Actors

III.1.4 Taxonomy of Risks in Cloud Networks

Clarke (2010) states that the risks of cloud computing are similar to those of in-house operations yet more opaque. Grobauer et al. (2011) propose a taxonomy of the general term risk, which implies "loss event frequency and probable loss magnitude". Many authors examine the risks of cloud computing but only a few address risks in cloud networks. Nevertheless, these examinations described below serve as a solid basis for our taxonomy of risks in cloud networks. Clarke (2012a) provides a checklist that lists risks and benefits of cloud computing in sub-categories. The author distinguishes between operational, contingent, security, commercial, and compliance risks. Troshani et al. (2011) divide cloud failure risks in technical risks, like data transit risk or malicious activities, and organizational risks, like lock-in or security and privacy risks. Jansen (2011) identifies six key security issues, namely trust, architecture, identity management, software isolation, data protection and availability, while explicitly describing cascading outages in cloud networks in the latter case. AlZain et al. (2012) identify three main cloud security risks, namely data integrity, data intrusion, and service availability. Armbrust et al. (2009) discuss obstacles for cloud computing, including for example the availability of the service, data lock-in, data confidentiality and auditability, data transfer bottlenecks, performance unpredictability, or reputation fate sharing. Moreover, Clarke (2012b) examines real world cloud reliability issues from 2005-2011.

Again, we take a look at the areas of supply chain networks and the financial industry. Regarding supply chain networks, Hallikas et al. (2004) identify the four types of risks "too low or inappropriate demand", "problems in fulfilling customer deliveries", "cost management and pricing", and "weakness in resources, development, and flexibility". For cloud networks, we can adopt the risk of shifts in demand and of a lack of flexibility. Prater (2005) distinguishes

between eight uncertainty factors. From that, we borrow "variable uncertainty" which covers factors such as weather, market behavior, or political influence factors. We also adopt the described parallel supply chain effects that refer to the dependency on several input goods with the possibility of missing input. In addition, chaotic demand peaks can be caused by wrongly conditioned enterprise resource planning (ERP) systems. This may also be relevant for cloud networks. In the financial industry, the term risk refers especially to "uncertain environmental variables that reduce performance predictability, as well as the lack of predictability in firm outcomes itself" (Miller 1992). These variables encompass general environmental, industry, and firm-specific risks (Miller 1992). Many of the thereby included risks are also found in literature on cloud risks, especially legal uncertainties (Armbrust et al. 2010; Jansen 2011) and input market specific uncertainties such as outages (Armbrust et al. 2010; Chow et al. 2009; Clarke 2010; Jansen 2011). In addition, we adopt the risk of unexpected demand shifts or price changes from the financial industry.

The literature on cloud computing does not use the term risk uniformly. In order to create a taxonomy of risks, we refer to Kaplan and Garrick (1981) who differentiate between *Hazard* and *Risk*. We adopt this "cause-and-effect" view for our taxonomy:

- A *Hazard* describes the "source of danger" (Kaplan and Garrick 1981). It strikes directly at a specific actor and affects its service. The thereby caused resulting *Risk* is measurable at the actor's customers, which are, for example, unable to use the respective cloud service as an input factor. The likelihood of the occurrence of a *Hazard* may be influenced by safeguards.
- A *Risk* "involves both uncertainty and some kind of loss or damage that might be received" (Kaplan and Garrick 1981).
- In addition to *Hazards* and *Risks*, we introduce *Reinforcers*, which are caused by the underlying network structure and can alter the measurable *Risks*.

Companies are mostly concerned about securing supply and steady prices of their pre-products. The derived basic risks are *Supply Risk* and *Price Risk*, whereas the *Supply Risk* in cloud computing can be divided in *Loss of Data* and *Availability Issues*. In addition to these two *Risks*, we consider *Data Issues* because the transferred good is information. We divide *Data Issues* in *Data Security* and *Data Privacy*. *Hazards* mostly describe the "traditional risks" of cloud computing like *Technical Defects*, yet also include *Shifts in Demand and Supply*, which may be provoked by strategic decisions of companies. *Reinforcers* include network specific circumstances that become relevant if risks occur. In addition, *Automation Errors* in service

provisioning systems may also intensify other risks. We use the term *Challenges* as a super-category for *Hazards*, *Risks*, and *Reinforcers* as these three categories represent challenges for a risk management in cloud networks. In order to address research question *RQ2*, we display the hierarchical taxonomy of risks in a UML class diagram with all identified *Hazards*, *Risks*, and *Reinforcers* in figure Abb. III-2. All sub-classes inherit from their super-classes. It can be read as follows: *Data Security* is a *Data Issue* is a *Risk* is a *Challenge*. We provide further information on all classes in table Tab. III-2 in the appendix.

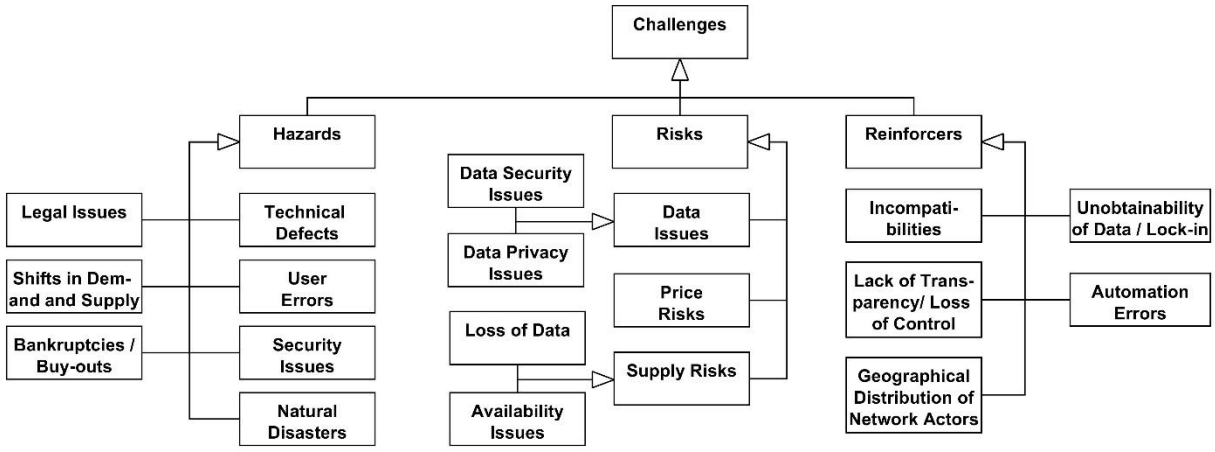

Abb. III-2 Taxonomy of Risks

III.1.5 Developing the Reference Model

We now construct the reference model, which is based on the taxonomies, in the following three steps: First, we identify the *Connections* between *Actors* in cloud networks that span a network, in a partial model. Second, we identify the causalities between *Hazards*, *Risks*, and *Reinforcers* in a partial model. Third, we assign the *Hazards*, *Risks*, and *Reinforcers* to specific *Actors* and display the possible dissemination of risks through a spanned network.

We constitute that the network consists solely of *Actors* and *Connections* between these *Actors*. In our reference model, *Actors* and *Connections* are vital parts of the network and do not exist without the network, which is displayed with the use of compositions. Further, in reality, one *Company* might appear as various *Actors* due to a manifold cloud service offering, which is again displayed with the use of a composition. Google, for example, acts as *Initial Application Provider* (GMail), *Initial Platform Provider* (Google App Engine), and as *Aggregator* (Google

News). The *Connection* symbolizes the "uses a service from" (from the perspective of a customer) or "service is used by" (from the perspective of a vendor) relation between a vendor and a customer. Our identified structure in the reference model implicates the assumption that an *Actor* usually does not consume a service and provides it without processing. This assumption is based on the existence of administration costs that raise the price of the actor's product above the price of the original product. The *Connections* between the respective actor classes at the position layer are represented by association classes. In order to guarantee easy readability, we removed the cardinalities from the association classes. All *Connections* represent *n-m* relationships between the respective *Actors*. From this it follows that one *Actor* can provide a service for various other *Actors* (a very common case) and various *Actors* can provide services for one *Actor* (allowing for the depiction of diversification strategies using backup/failover providers). Below this abstraction layer, the *Actors* do not behave differently in terms of their interaction. In figure Abb. III-3, we illustrate the partial model of actors in cloud networks.

As clarified above, *Hazards* describe the cause of a *Risk*, whereas *Reinforcers* may increase the damage or the probability of a *Risk*. A *Risk* can be caused by various *Hazards* and a *Hazard* can cause several *Risks*, which equals an *n-m* relationship. Again, we removed these cardinalities from the association class to guarantee easy readability. The same is valid for the "cause-and-effect" relationship between *Reinforcers* and *Risks*. The sub-classes of *Hazards*, *Risks*, and *Reinforcers* inherit this feature from their super-classes. However, *Hazards* and *Reinforcers* have different effects on different *Risks*. For example, the *Incompability* cannot reinforce the *Data Security Issues*. In table Tab. III-3 and table Tab. III-4 in the appendix, we illustrate the possible combinations which have been elaborated by our own critical reflection. In figure Abb. III-4, we illustrate the partial model of challenges.

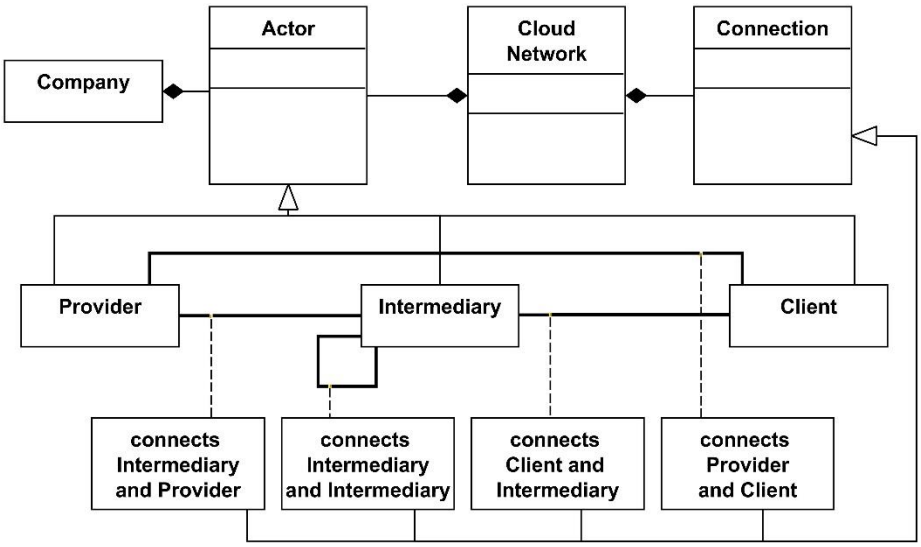

Abb. III-3 Partial Model of Actors in Cloud Networks

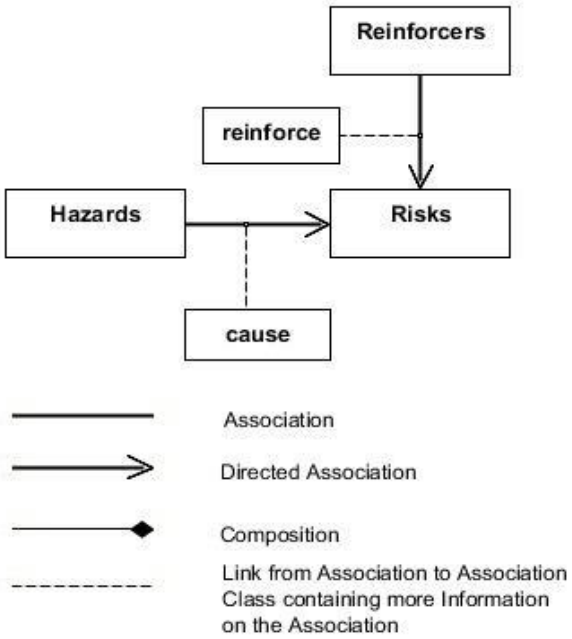

Abb. III-4 Partial Model of Challenges

We join the two partial models to a reference model. We illustrate the dependencies between *Risks* and *Hazards*/*Reinforcers* as association classes. A basic characteristic of our reference model is that *Risks* can be disseminated from one *Actor* to another through a specific *Connection*. Generally, *Risks* are disseminated from vendor to customer. This dissemination is represented in our reference model through methods in the *Connection* class. Specific *Hazards* strike at specific *Actors* in the cloud network. Also, specific *Risks* can be detected at specific *Actors* in the cloud network. Therefore we assign the *Risks* and *Hazards* classes to the *Actor* class. The *Reinforcers* are determined by the class *Cloud Network*.

A *Hazard* strikes at a specific *Actor* and therefore affects the *Actor's* cloud service output. The *Actor's* customers using this service as input are able to measure the thereby caused *Risk*. If this *Risk* affects the cloud service output of the customer, the *Risk* is in turn disseminated to the customer's customer which again can detect the *Risk*. For example, in case of a *Technical Defect* at the *Initial Platform Provider* A, A fails to deliver the service correctly. Therefore *Application Reseller* B using this service can detect *Availability Issues* such as outages or bad performance. The *Availability Issue* may also affect the produced application services by B and in turn be disseminated to *Aggregator* C which uses B's service for the assembly of its own offerings. At B and C, the *Risk* might even be worsened through a *Lock-In*. In figure Abb. III-5, we illustrate the developed final reference model.

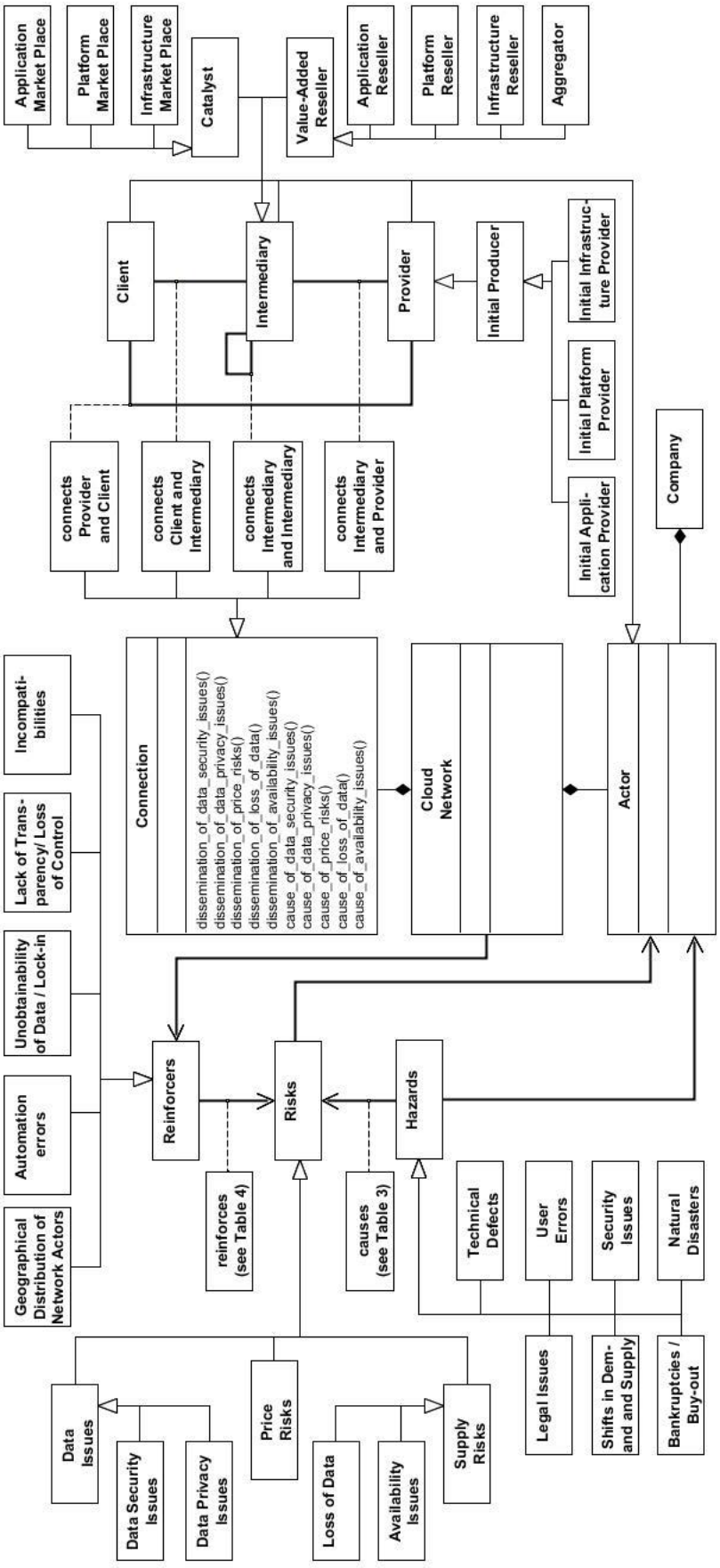

Abb. III-5 Reference Model to Support Risk Identification in Cloud Networks

III.1.6 Evaluation

As proposed by Schuette and Rotthowe (1998), our artifact is based on the body of existing literature in the field of cloud computing and other relevant disciplines. We constructed two taxonomies and used them as the foundation for our reference model. To evaluate our findings, we first evaluated the individual taxonomies. Second, we evaluated the reference model. For this purpose we applied a "multi-method" approach (Martens and Teuteberg 2011). For the taxonomies we used real world examples and, in accordance with Gregor and Hevner (2013), conducted semi-structured interviews with industry experts from focus group companies. For the reference model, we again conducted interviews with the industry experts and additionally instantiated the reference model with real world actors to demonstrate its applicability. We critically discussed any feedback received in the interviews with other researchers before incorporating it into our models, presented in the sections above.

For interviewee selection, we identified possible interview partners that (i) represented different kinds of actors in cloud networks and therefore covered a "wide spectrum of expert knowledge" (Martens and Teuteberg 2011) and (ii) could be considered "domain experts" with "expertise in the cloud computing area" (Boehm et al. 2010) due to holding important positions with several years of experience in the respective companies. We were able to conduct interviews with two available interviewees from two different companies. Their diverse business models and perspectives on cloud computing support a reasonable generalizability of our reference model. Our first interview partner is the CEO of company X. This company is a small sized customizing partner of Y, one of the world's largest SaaS ERP providers, and uses several cloud-based third-party add-ins which offer specific functionalities. Y hosts its services in the United States, whereas company X is located in Germany. The interview partner has extensive knowledge regarding dependencies among cloud services through several years of experience in customizing SaaS services for X's customers. Our second interview partner is the Head of IT Architecture of Company Z. This company is one of the world's largest, globally acting IT service providers. Offerings range from IaaS to SaaS in trusted public, private, and hybrid cloud environments for large commercial and governmental organizations. During the last year, the company invested approximately 2 billion dollar in their cloud-based developments. The interview partner has profound knowledge in the field of cloud services through years of experience in purchasing cloud services for the internal use in company Z, as well as through responsibility for the availability of the necessary IT resources for external cloud service consumers.

Concerning the problem relevance, both interview partners confirmed the developments towards cloud networks as well as the resulting lack of transparency and newly emerging risks. They particularly underlined the trend towards standardization of infrastructure services. Company X's customers consider availability and geographical location of the stored data to be main concerns. Many customers therefore implement local safeguards such as physically independent internet connections. However, the customers of company X do not usually address cloud network related risks. Company Z considers the loss of data and outages of cloud services to be major concerns. They propose multi-vendor sourcing and detailed service level agreements as safeguards to cope with these issues.

III.1.6.1 Evaluation of the Taxonomies

We discussed our taxonomies with the industry experts from company X and Z. We then incorporated the respective gained insights into the taxonomies. In the following, we illustrate some annotations of the experts with regard to our former artifacts:

- An interview partner noted that many companies in cloud networks might appear as various *Actors* at the same time. To overcome this issue, we came up with the class *Company* that consists of *1-n Actors*.
- Regarding the taxonomy of risks in cloud networks, an interview partner felt that a formerly depicted hazard *Bad Reputation* is a type of *Demand Risk*.
- Another issue was that our former distinction of *Data Issues* was not exact enough. Hence, we divided the respective risk *Data Security* (now *Data Issues*) into *Data Security* and *Data Privacy*.
- An interview partner remarked that performance issues could be a cause of a *Supply Risk*. We followed this advice by renaming the *Risk Outages* to *Availability Issues* which now also contains performance issues.
- Both interview partners confirmed the completeness of the taxonomy of actors and risks in cloud networks for their purposes and based on their expertise. Furthermore, all changes were discussed with other researchers.

In addition, we applied a conceptual to empirical approach described by Nickerson et al. (2013) during the construction of our taxonomies, which includes an evaluation through the identification of real world examples for the illustrated sub-classes. After several cycles of elaborating our taxonomies, we sufficiently matched the objective and subjective ending conditions described by Nickerson et al. (2013). Regarding the objective ending condition

"every characteristic must be explained by an example", we could not find real world examples for the risks *Price Risk* and *Data Security Issues*. Information about such problems does usually not go public. However, the interview partners confirmed the existence of these risks. We could also not find real world examples for *Infrastructure Reseller* and *Platform Market Place*. As the developments towards cloud networks are still ongoing, not every described actor is already in business and therefore cannot be observed right now. However, our models are meant to include near future market structures in cloud computing. Therefore, we tried to explain circumstances under which such actors may likely exist in the near future. The interview partners confirmed the high likeliness of these actors. In addition to these objective ending conditions, we and our interview partners felt that the taxonomies had reached a state where they now were concise, robust, comprehensive, extendible, and explanatory (subjective ending condition). In table Tab. III-1 in the appendix, we illustrate the actors of cloud networks with a textual description and the identified real world examples. In table Tab. III-2 of the appendix, we illustrate the risks of cloud networks with a textual description and the identified real world examples.

III.1.6.2 Evaluation of the Reference Model

We discussed our reference model with the industry experts from company X and Z. Again, we then incorporated the respective gained insights into the reference model. In the following, we illustrate some annotations of the experts with regard to our former artifact:

- An interview partner annotated that the former illustration was very complex and required a long settling-in period. We were able to simplify the illustration by moving the direct connections between the actors and the associated risks into the association classes, which are now displayed in table Tab. III-3 and table Tab. III-4 in the appendix. The new illustration now allows an easier and more comprehensive adaption by practitioners without losing too much expressiveness in its depiction.
- A former version of our reference model allowed actors to disseminate hazards to other actors. An interview partner suggested that we should consider the dissemination of the respective risk itself. After discussions with other researchers we adopted this suggestion and adjusted our reference model accordingly.
- Both interview partners developed a good understanding of the reference model and described it as reasonable and applicable. Furthermore, all changes were discussed with other researchers.

Next, we demonstrate the applicability of our reference model by instantiating it with real world actors. In order to remain consistent with the UML class diagram, we use an UML object diagram. We chose the already described dependencies between Amazon EC2 and Microsoft Yammer and expanded it with SAP Spotlight which is another customer of Crocodoc. In our example, we look at a *Client* "ACME" which consumes services of the two *Application Resellers* Yammer and SAP Spotlight to support its business operations. We assume that the datacenters of Amazon and Microsoft are located in the same area and therefore are both affected by a blackout due to a lightning storm (*Natural Disaster*). Subsequently, Amazon causes risks (*Price Risk*, *Loss of Data*, and *Availability Issues*) at their customer Crocodoc that in turn disseminates the risks to its customers Yammer and SAP Spotlight. Yammer and Spotlight are able to measure these *Risks* that affect their service input. At the same time, the affected Microsoft Servers cause *Risks* (*Price Risk*, *Loss of Data*, and *Availability Issues*) at Yammer. As Yammer consumes services from Amazon EC2 and the Microsoft Servers, the *Hazard* affects Yammer even more. We speak of the *Reinforcer* "*Geological Distribution of Network Actors*". This *Reinforcer* worsens the magnitude of Yammer's *Risks*. In the following, the *Risks* at Yammer and SAP Spotlight are disseminated through the cloud network until the last node (company ACME) is affected. In addition, we assume a user mistake (*User Error*) at SAP Spotlight. Therefore, this actor also causes *Risks* (*Loss of Data*, *Availability Issues*, *Data Security*, and *Data Privacy*) at company ACME. These *Risks* add up to the *Risks* disseminated from the lightning storm (*Price Risk*, *Loss of Data*, and *Availability Issues*). We illustrate this instantiation of our reference model in figure Abb. III-6. The depicted model provides transparency on the existing dependencies. The dissemination of risks through the cloud network can be displayed and the respective actors are able to identify the impending risks.

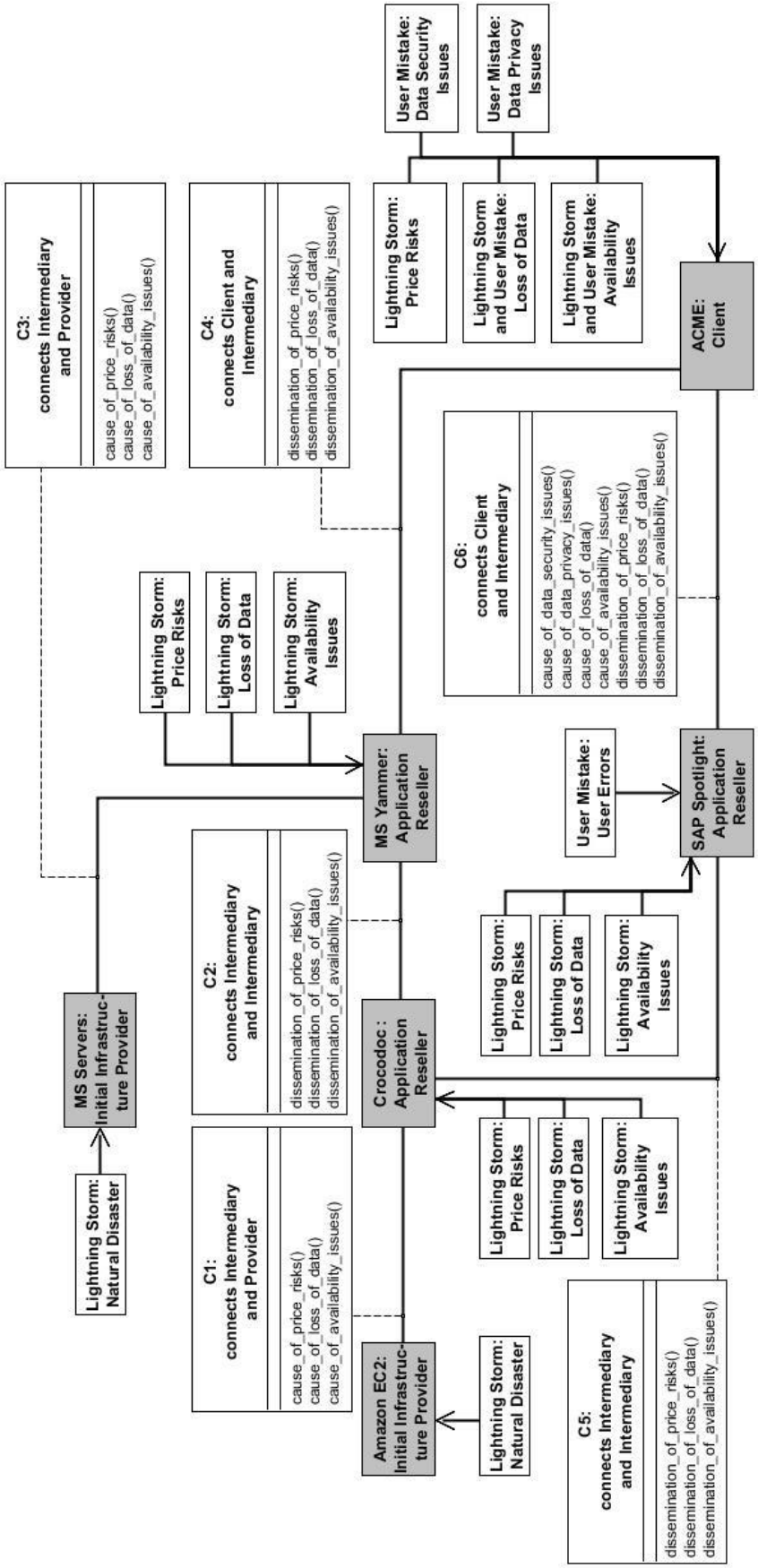

Abb. III-6 Instantiation of the Reference Model

III.1.7 Implications, Applicability, and Future Research

In our paper, we describe ongoing developments in cloud computing, such as standardization, specialization, rising dependencies, new actors, and new market structures. These developments are likely to transform the current cloud landscape into complex, globally distributed cloud networks with new emerging risks. In order to provide a better understanding of the underlying structure and the inherent risks, we develop taxonomies of actors and risks in cloud networks (*RQ1* and *RQ2*). On this basis, we build a reference model based on UML class diagrams that can be instantiated and supports risk identification in cloud networks. We evaluate the taxonomies and the reference model through real world examples and interviews with industry experts.

Cloud networks are participant governed networks in which, regarding governance, no clear responsibilities are yet determined. As cloud networks become more complex and the number of participants increases, there is a need for cloud network governance which, considering the research of Provan and Kenis (2007), might be best addressed by a network administrative organization. Zissis and Lekkas (2012) also propose a trusted third party to enforce cloud governance. However, as the implementation of an institution that will provide a holistic cloud network governance may need some years, practitioners need to address the prevailing risks on their own in the meantime. In both ways, clear defined cloud network governance principles and processes are needed. Therefore, existing approaches from a single company view may be adapted, e.g. Guo et al. (2010) or Zhang et al. (2010). Also, existing knowledge on network governance (e.g. Jones et al. 1997 and Provian and Kenis 2007) or supply chain governance (e.g. Bitran et al. 2006, Gereffi et al. 2005, Richley et al. 2010, and Wathne and Heide 2004) could be incorporated.

Following the risk cycle of Zhang et al. (2010), which is based in the NIST Risk management guide (Stoneburner et al. 2002), risk analysis (or risk identification) is an essential step in terms of risk management and should also be part of risk management in a network (Hallikas et al. 2004). The reference model could be applied by practitioners in terms of a government process that coordinates “cloud-based services management and policy implement across the enterprise” (Guo et al. 2010). More specific, the reference model enables practitioners to select relevant critical areas and identify the respective occurring risks (Zhang et al. 2010). In addition, it provides a depiction of actors in the cloud network and thereby the implementation of “threat identification” (Zhang et al. 2010). Concluding, the reference model provides practitioners and

researchers with a better understanding of the nexus of cloud networks and related risks, thereby supporting risk identification:

- Relevant actors and structures in cloud networks can be displayed and thereby impending risks can be identified.
- The dissemination of risks throughout cloud networks can be examined.

Considering its application, responsibility for instantiating the reference model in the course of implementing cloud network governance structures lies with the individual participants of the cloud network for now. To instantiate the reference model for their own specific eco-system, practitioners need to gather information on actors and hazards. Similar to the existence of industry-specific associations in supply chains like e.g. the automotive industry, which provide information on possible suppliers (Choi and Hartley 1996), cloud industry-specific associations may arise in the future which might be used for information gathering on relevant actors. In addition, information on actors can originate from information pages of respective actors, from communication with respective actors, from cloud marketplace directories (e.g. Amazon Web Services Marketplace 2014), or from publicly available research results (e.g. CloudServiceMarket 2014). In the future, there may be some kind of automated information interchange on the underlying network as it is already practiced in supply chain networks today (compare Spekman et al. 1998). Information on hazards may be a bit harder to obtain as cloud actors have no interest in making these events publicly available. Hence, our taxonomy of risks could be used as a guideline for examining possible hazards. Also, cloud industry-specific media reports on past events might serve as an indicator for prevailing hazards. We argue, that even the instantiation with limited obtainable information in a rather small cloud eco-system should provide added value in terms of risk management in cloud networks as it will shed some light on at least a part of the existing risks, thereby making risk mitigation possible. Yet, the development of a detailed risk analysis process for cloud network governance, including the reference model as a necessary step, is subject to further research.

Cloud computing is a highly dynamic market. Many new market structures and challenges may change during the next several years. Therefore the validity of our current model cannot be guaranteed for the future and will be subject to continuous adjustment and development. Furthermore, as of now, we have only modeled one real-world example. In future research, we will collaborate with more practitioners and experts in order to further examine relevant actors and challenges and to display more partial cloud networks. These partial views could be connected to a large “cloud network map” that displays the dependencies among many existing

cloud actors. With the identified causalities between hazards, risks, and reinforcers and the identified dissemination of risks modeled as a semi-formal diagram, we have set a basis for risk quantification approaches. In the next step, we will apply existing criticality measures to identify the key actors in cloud networks. Subsequently, we want to develop new cloud network specific risk measures and our reference model could serve as a basis for the development of an IT tool for risk quantification. The estimation of possible input values for this tool could be subject to future empirical research. After gaining knowledge on existing risks and their possible impact, we are planning on developing and evaluating safeguards addressing the identified risks. Thereby, the effect of different types of risks and actors on the respective appropriate risk management strategy could also be investigated further.

III.1.8 References

AlZain, M. A., Pardede, E., Soh, B., and Thom, J. A. 2012. "Cloud computing security: from single to multi-clouds," in *45th Hawaii International Conference on System Sciences*, Maui, pp. 5490-5499.

Amazon Web Services Marketplace 2014. "AWS Marketplace," https://aws.amazon.com/marketplace. Visited: August 13th 2014.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., and Stoica, I. 2009. "Above the Clouds: A Berkeley View of Cloud Computing," *Technical Report UCB/EECS-2009-28, University of California, Berkeley*, pp. 1-23.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., and Stoica, I. 2010. "A view of cloud computing," *Communications of the ACM* (4:53), pp. 50-58.

Bitran, G., Gurumurthi, S., and Sam, S. 2006. "Emerging Trends in Supply Chain Governance," *MIT Sloan School of Management Working Report Paper 227*, pp. 1-33.

Bleizeffer, T., Calcaterra, J., Nair, D., Rendahl, R., Schmidt-Wesche, B., and Sohn, P. 2011. "Description and application of core cloud user roles," in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, Cambridge, pp. 1-9.

Blue, V. 2013. "Find out if your data was leaked in the Adobe hack," http://www.zdnet.com/find-out-if-your-data-was-leaked-in-the-adobe-hack-7000023065/. Visited: August 13th 2014.

Bresnahan, J., Keahey, K., LaBissoniere, D., and Freeman, T. 2011. "Cumulus: an open source storage cloud for science," in *Proceedings of the 2nd International Workshop on Scientific Cloud Computing*, San Jose, pp. 25-32.

Buyya, R., Yeo, C. S., and Venugopal, S. 2008. "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," in *10th IEEE International Conference on High Performance Computing and Communications*, Dalian, pp. 5-13.

Böhm, M., Koleva, G., Leimeister, S., Riedl, C., and Krcmar, H. 2010. "Towards a generic value network for cloud computing," in *Economics of Grids, Clouds, Systems, and Services*, Jörn Altmann and O. F. Rana (eds.) Springer, pp. 129-140.

Choi, T., and Hartley, H. 1996. "An exploration of supplier selection practices across the supply chain," *Journal of Operations Management* (4:14), pp. 333-343.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., and Molina, J. 2009. "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud Computing Security*, Chicago, pp. 85-90.

Clarke, R. 2010. "Computing clouds on the horizon? Benefits and risks from the user's perspective," in *23rd Bled eConference*, Bled, pp. 569-590.

Clarke, R. 2012a. "A Framework for the evaluation of cloudsourcing proposals," in *25th Bled Conference*, Bled, pp. 309-323.

Clarke, R. 2012b. "How reliable is cloudsourcing? A review of articles in the technical media 2005–11," *Computer Law & Security Review* (1:28), pp. 90-95.

Clemons, E. K., and Chen, Y. 2011. "Making the decision to contract for cloud services: managing the risk of an extreme form of IT outsourcing," in *44th Hawaii International Conference on System Sciences*, Manoa, pp. 1-10.

CloudServiceMarket 2014. "CloudServiceMarket," http://www.cloudservicemarket.info/. Visited: August 13th 2014.

Cloud Standards Customer Council 2014. "Cloud Standards Customer Council," http://www.cloud-council.org/. Visited: August 13th 2014.

Dillon, T., Wu, C., and Chang, E. 2010. "Cloud computing: issues and challenges," in *24th IEEE International Conference on Advanced Information Networking and Applications*, Perth, pp. 27-33.

Evolven 2012. "Downtime, Outages and Failures - Understanding their True Costs," http://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html. Visited: August 13th 2014.

Gereffi, G., Humphrey, J., Sturgeon T. 2005. "The governance of global value chains," *Review of International Political Economy* (1:12), pp. 78-104.

Gregor, S., and Hevner, A. R. 2013. "Positioning and presenting design science research for maximum impact," *Management Information Systems Quarterly* (2:37), pp. 337-355.

Grobauer, B., Walloschek, T., and Stocker, E. 2011. "Understanding cloud computing vulnerabilities," *IEEE Security & Privacy* (2:9), pp. 50-57.

Guo, Z., Song, M., and Song, J. 2010. "A Governance Model for Cloud Computing," in *International Conference on Management and Service Science*, Wuhan, pp. 1-6.

Hallikas, J., Virolainen, V., and Tuominen, M. 2002. "Risk analysis and assess- ment in network environments: a dyadic case study," *International Journal of Production Economics* (1:78), pp. 45-55.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V., and Tuominen, M. 2004. "Risk management processes in supplier networks," *International Journal of Production Economics* (1:90), pp. 47-58.

Harland, C. M. 1996. "Supply chain management: relationships, chains and networks," *British Journal of Management* (1:7), pp. 63-80.

Harnisch, S., and Buxmann, P. 2013. "Evaluating Cloud Services Using Methods of Supplier Selection," in *Business Information Systems*, Poznan, pp. 1-13.

Harris, D. 2011. "Cloud Platforms Heroku, DotCloud & EngineYard Hit Hard By Amazon Outage," http://gigaom.com/2011/04/21/more-than-100-sites-went-down-with-ec2-including-your-paas-provider/. Visited: August 13th 2014.

Harris, D. 2014. "Did google just doom the lot of small-scale cloud providers?" http://gigaom.com/2014/03/29/did-google-just-doom-the-lot-of-small-scale-cloud-providers/. Visited: August 13th 2014.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," *Management Information Systems Quarterly* (1:28), pp. 75-106.

Höfer, C., and Karagiannis, G. 2010. "Taxonomy of cloud computing services," in *IEEE GLOBECOM Workshops*, Miami, pp. 1345-1350.

Höfer, C., and Karagiannis, G. 2011. "Cloud computing services: taxonomy and comparison," *Journal of Internet Services and Applications* (2:2), pp. 81-94.

IDC 2013. "IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation," http://www.idc.com/getdoc.jsp?containerId=prUS24298013. Visited: August 13th 2014.

Jaeger, P. T., Lin, J., and Grimes, J. M. 2008. "Cloud Computing and Information Policy: Computing in a Policy Cloud?," *Journal of Information Technology & Politics* (5:3), pp. 269-283.

Jansen, W. A. 2011. "Cloud hooks: Security and privacy issues in cloud computing," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, Manoa, pp. 1-10.

Jones, C., Hesterly, W., and Borgatti S. 1997. "A General Theory of Network Governance: Exchange Conditions and Social Mechanisms," *The Academy of Management Review* (4:22), pp. 911-945.

Kaplan, S., and Garrick, B. J. 1981. "On the quantitative definition of risk," *Risk Analysis* (1:1), pp. 11-27.

Knackstedt, R., Lis, L., Stein, A., Barth, I., and Becker, J. 2009. "Towards a reference model for online research maps," in *Proceedings of the 17th European Conference on Information Systems*, Verona, pp. 2315-2326.

König, C., Mette, P., and Müller, H. 2013. "Multivendor portfolio strategies in cloud computing," in *Proceedings of the 21st European Conference on Information Systems*, Utrecht, pp. 1-12.

Lambert, D. M., Cooper, M. C., and Pagh, J. D. 1998. "Supply chain management: implementation issues and research opportunities," *The International Journal of Logistics Management* (2:9), pp. 1-20.

Laurent, O. 2013. "EyeEm photo-sharing app aims to enable photographers to sell their images," British Journal of Photography. http://www.bjp-online.com/2013/04/eyeem-photo-sharing-app-aims-to-enable-photographers-to-sell-their-images/. Visited: August 13th 2014.

Leavitt, N. 2009. "Is Cloud Computing Really Ready for Prime Time?" *Computer* (1:42), pp. 15-20.

Leimeister, S., Riedl, C., Böhm, M., and Krcmar, H. 2010. "The business perspective of cloud computing: actors, roles, and value networks," in *Proceedings of 18th European Conference on Information Systems*, Pretoria, pp. 1-12.

Linden, A., and Fenn, J. 2003. "Understanding Gartner's hype cycles," *Strategic Analysis Report Nº R-20-1971. Gartner Inc*, pp. 1-12.

Marinos, A., and Briscoe, G. 2009. "Community cloud computing," in *Proceedings of the 1st International Conference on Cloud Computing*, Beijing, pp. 472-484.

Martens, B., and Teuteberg, F. 2011. "Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model." in *17th Americas Conference on Information Systems*, Detroit, pp. 1-10.

Miller, K. D. 1992. "A framework for integrated risk management in international business," *Journal of International Business Studies* (2:23), pp. 311-331.

Miller, R. 2011. "Outage in Dublin Knocks Amazon, Microsoft Data Centers Offline," http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/. Visited: August 13th 2014.

Nickerson, R. C., Varshney, U., and Muntermann, J. 2013. "A method for taxonomy development and its application in information systems," *European Journal of Information Systems* (3:22), pp. 336-359.

OMG 2011. "UML 2.4.1 Superstructure," http://www.omg.org/spec/UML/2.4.1/Superstructure/PDF/. Visited: August 13th 2014.

Paternò, F., and Santoro, C. 2002. "Preventing user errors by systematic analysis of deviations from the system task model," *International Journal of Human-Computer Studies* (2:56), pp. 225-245.

Prater, E. 2005. "A framework for understanding the interaction of uncertainty and information systems on supply chains," *International Journal of Physical Distribution & Logistics Management* (7:35), pp. 524-539.

Provian, K., and Kenis, P. 2007. “Modes of Network Governance: Structure, Management, and Effectiveness,” *Journal of Public Administration Research and Theory* (2:18), pp. 229-252.

Richley, G., Roath, A., and Whipple, J. 2010. “Exploring a Governance Theory of Supply Chain Management: Barriers and Facilitators to Integration,” *Journal of Business Logistics* (1:31), pp. 237-256.

Rimal, B. P., Choi, E., and Lumb, I. 2009. "A taxonomy and survey of cloud computing systems," in *5th International Joint Conference on INC, IMS and IDC*, Seoul, pp. 44-51.

Saripalli, P., and Walters, B. 2010. "Quirc: A quantitative impact and risk assessment framework for cloud security," in *Proceedings of the 3rd International Conference on Cloud Computing*, Miami, pp. 280-288.

Schuette, R., and Rotthowe, T. 1998. "The guidelines of modeling–an approach to enhance the quality in information models," *in Conceptual Modeling–ER'98*, Tok-Wang Ling, S. Ram and M. L. Lee (eds.) Springer, pp. 240-254.

Spekman, R., Kamauff, J., and Myhr, N. 1998. „An Empirical Investigation into Supply Chain Management – A Perspective on Partnerships,” *Supply Chain Management* (2:3), pp. 53-67.

Stoneburner, G., Goguen, A., and Feringa, A. 2002. "Risk management guide for information technology systems," *NIST special publication 800-30*, pp. 1-56.

Troshani, I., Rampersad, G., and Wickramasinghe, N. 2011. "On Cloud Nine? An Integrative Risk Management Framework for Cloud," in *24th Bled Conference*, Bled, pp. 15-26.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. 2009. "A Break in the Clouds: Towards a Cloud Definition," *ACM SIGCOMM Computer Communication Review* (1:39), pp. 50-55.

Vom Brocke, J., and Thomas, O. 2006. "Reference Modeling for Organizational Change: Applying Collaborative Techniques for Business Engineering." in *Proceedings of the 12th Americas Conference on Information Systems*, Acapulco, pp. 680-688.

Wathne, K., and Heide, J. 2004. “Relationship Governance in a Supply Chain Network,” *Journal of Marketing* (1:68), pp. 73-89.

Youseff, L., Butrico, M., and Da Silva, D. 2008. "Toward a unified ontology of cloud computing," in *Grid Computing Environments Workshop*, Austin, pp. 1-10.

Zhang, X., Wuwong, N., Li, H., and Zhang, X. 2010. "Information security risk management framework for the cloud computing environments," in *10th International Conference on Computer and Information Technology*, Bradford, pp. 1328-1334.

Zissis, D., and Lekkas, D. 2012. "Addressing cloud computing security issues," *Future Generation Computer Systems* (3:28), pp. 583-592.

III.1.9 Appendix

Actor			Description
Provider	Initial Producer	Initial Application Provider	Applications encompass software, web apps, or internet services, often summarized as SaaS, which are developed and made available on the provider's own infrastructure. The Initial Application Provider provides the "appropriate hardware and software infrastructure to run the service and the people to manage and maintain this infrastructure" (Bleizeffer et al. 2011). Services are provided to *0…n* Intermediaries and *0…n* Clients. *Examples: Microsoft Office 365, Google Mail.*
		Initial Platform Provider	Initial Platform Providers offer an "environment within which cloud applications can be deployed" (Leimeister et al. 2010), including an operating environment, application programming interfaces (APIs), programming languages and so on (Boehm et al. 2010). The Initial Platform Provider uses its own infrastructure to provide its platform. Services are provided to *0…n* Intermediaries and *0…n* Clients. *Examples: Microsoft Windows Azure, Google App Engine.*
		Initial Infrastructure Provider	Initial Infrastructure Providers provide IT resources such as "storing and processing capacity" (Vaquero et al. 2008). They are usually "companies with other web activities that require large computing resources" (Marinos and Briscoe 2009) and benefit from its economies of scale. Subcategories are the Initial Computing Provider and the Initial Storage Provider. Both provide services to *0…n* Intermediaries and *0…n* Clients. *Initial Computing Provider: Amazon EC2, Rackspace Cloud Servers.* *Initial Storage Provider: Amazon S3, Rackspace Cloud Databases.*

Intermediary	Value-Added Reseller	Application Reseller	The output of an Application Reseller is similar to the output of an Initial Application Provider, whereas the Application Reseller accesses services which encompass "hardware and infrastructure of the infrastructure providers" (Leimeister et al. 2010) or other application or platform services as pre-products and "adds value on top of a given service to ensure some specific capability" (Boehm et al. 2010). However, today's most common form is a self-hosted service that consumes other services as add-ins. An Application Reseller provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0…n* Providers and *0…n* Intermediaries. *Examples: Crocodoc, Netflix, Talentsoft.*
		Platform Reseller	The output of a Platform Reseller is similar to the output of an Initial Platform Provider, whereas the Platform Reseller accesses computing power or data storage of the Initial Infrastructure Providers or other platform services as pre-products. A Platform Reseller provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0...n* Providers and *0…n* Intermediaries. *Examples: Heroku, Bitbucket.*
		Infrastructure Reseller	The Infrastructure Reseller buys and sells infrastructure services. It is a virtual actor and nowadays may not exist. Infrastructure is a standardized commodity thus value can't be added. Markets of commodities are usually liquid and buying and selling an identical service leads to losses due to transaction costs. The optimization of load balancing between internal and external resources, as described by Armbrust et al. (2009), may be a special case when the reselling of infrastructure makes economic sense. An Infrastructure Reseller provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0...n* Providers and *0…n* Intermediaries. *We are not able to show this actor in a real world example due to missing insight in the internal optimization of Initial Infrastructure Providers. However, our interview partners confirmed the likeliness of its (future) existence.*

		Aggregator	An Aggregator generates value through the aggregation of services without adding new functionalities to existing services. The Aggregator ensures "that the different services work together neatly and that no losses occur via data movement between the systems" (Boehm et al. 2010). An Aggregator provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0...n* Providers and *0…n* Intermediaries. *Examples: HP Aggregation Platform for SaaS, Zapier.*
	Catalyst	Application Market Place	An Application Market Place matches customer demand with vendor offerings. Its main objective is to "bring customers and service providers together" (Boehm et al. 2010). It offers decision support for the customer through comparing various cloud services "based on certain selection criteria" (Boehm et al. 2010). The Application Market Place could offer additional benefits to both service providers and customers, such as SLA contracting or billing (Boehm et al. 2010). An Application Market Place links services of *0…n* Intermediaries or *0…n* Providers to *0...n* Intermediaries or *0…n* Clients. Independent from this, the Application Market Place may use services of 0…n Intermediaries or *0…n* Providers to run its own service. *Examples are VMware vCloud Hybrid Service Online Marketplace, Salesforce AppExchange.*
		Platform Market Place	A Platform Market Place is similar to the Application Market Place. However, the trading object encompasses platform services. Therefore a Platform Market Place links services of 0…n Intermediaries or *0…n* Providers to *0...n* Intermediaries or *0…n* Clients. Independent from this, the Platform Market Place may use services of *0…n* Intermediaries or *0…n* Providers to run its own service. *We are not able to show this actor in a real world example. However, our interview partners confirmed the likeliness of its future existence. For example, a platform market place could occur due to licensing of platforms such as Microsoft Azure by third party providers.*

		Infrastructure Market Place	An Infrastructure Market Place is similar to the Application Market Place. However, the trading object encompasses infrastructure services. Buyya et al. (2008) describe their vision of a cloud market with brokers that purchase cloud services for their customers. Due to high standardization, infrastructure exchanges may be compared to commodity exchanges which automatically map consumer demand with vendor offerings. An Infrastructure Market Place links services of *0…n* Intermediaries or *0…n* Providers to *0...n* Intermediaries or *0…n* Clients. Independent from this, the Infrastructure Market Place may use services of *o…n* Intermediaries or *o…n* Providers to run its own service. *Example: Deutsche Boerse Cloud Exchange.*
Client			A Client is "the starting point of a service request and the ending point of service delivery" (Boehm et al. 2010). The Client solely uses products produced by its vendors and consumes these products outside of the cloud network. A Client receives services from *0...n* Providers or *0…n* Intermediaries. *Clients mostly encompass "everyday users, Small and Medium sized Enterprises (SMEs), and ambitious start-ups" (Marinos and Briscoe 2009).*

Tab. III-1 Description of Actors

Challenge		Description
Risks	Availability Issues	Most customers worry about availability issues whereas cloud services have set new standards in high availability (Armbrust et al. 2010; Chow et al. 2009; Leavitt 2009). On the other hand, Jansen (2011) states that even a very high level of availability leads to a significant downtime over a year. That's why Clarke (2012a) describes that "outages are not uncommon, and they may last for some hours". In addition, Availability Issues also encompass connection interruptions and performance issues. We can distinguish between permanent and temporary availability issues (Clarke et al. 2010). *Amazon EC2 users were affected by an outage in 2011 Clarke (2012b).*
	Loss of Data	Loss of Data is permanent. In addition, a lack of data integrity describes "sustained correctness of the service, and of the data "Clarke (2012a). It can be compared to Loss of Data because the data is useless and is "harmful to the user and the users' customers" (Clarke 2010). Al Zain et al. (2012) state that data "can suffer from damage during the transition operations from or to the cloud storage". *Innocent companies were affected by an FBI raid in computing centers against a handful of companies that operated out of the centers (Jansen 2011).*
	Price Risks	Besides volatile prices, Price Risks include entry costs, switching costs, or operation costs (Clarke 2012a). Clarke (2010) states that customers are dependent on the prices of their vendors. In addition, the data transmission of large volumes is cost intensive (Clarke 2010). We also identified Price Risks in the literature on financial markets that may become more relevant with the ongoing drive for standardization and commoditization. *We are not able to show this risk in a real world example due to missing insights. However, our interview partners confirmed its existence.*

	Data Security Issues	Data Security Issues concern the security of the service itself and of company-related data. The size of a company has a huge impact on its Data Security, whereby large companies have higher investment volumes and therewith are generally more professional than small companies. However, they are more visible to attackers (Clarke 2010). Jansen (2011) states that data must not only be secured at rest but also when in transit and in use. *We are not able to show this risk in a real world example due to missing insights. However, our interview partners confirmed its existence.*
	Data Privacy Issues	Data Privacy Issues describe the risk of revelation of data that does not belong to the company itself, such as user data. Troshani et al. (2011) mention that besides security breaches, also privacy breaches "can result in serious economic loss". *Adobe was hacked in 2013 and over 100 million user data were revealed (Blue 2013).*
Hazards	Technical Defects	Technical Defects include, hardware, software, or network issues. In addition, Chow et al. (2009) state that some "third-party cloud would not scale well enough to handle certain applications". Cloud actors use redundancy in their technical infrastructure to improve the availability (Armbrust et al. 2010). *Virgin Blue's airline's check-in and online booking systems went down due to a hardware failure, on September 26, 2010 (Evolven 2012).*
	User Errors	User Errors involve issues such as erroneous entries of data or passwords that can be easily cracked and enable the access to data for outsiders. User Errors are no cloud specific risk and are widely discussed in existing literature, such as (Paternò and Santoro 2002). *Clarke (2012b) mentions a user mistake that led to an outage of "Amazon IaaS" in 2011.*

	Security Issues	Security Issues include, for example, fraud, hacking, or denial of service attacks (Grobauer et al. 2011) and originate from external attackers or from attacks within the company. Chow et al. (2009) state that sourcing into the cloud enlarges the attack surface of an actor. *An example for a security issues is the leak of a huge amount of authentication names and passwords of Adobe users (Blue 2013).*
	Natural Disasters	Natural Disasters that affect cloud actors may be, for example, earthquakes, floods, or extreme storms. Jansen (2011) mentions natural disasters as possible source of unplanned outages. *A lightning strike caused a power outage that led to an outage of datacenters of Amazon and Microsoft near Dublin (Miller 2011).*
	Shift in Demand or Supply	Actors can be affected by demand shifts, which may be caused by strategic decisions of companies, bad publicity, or an outage of a competitor. The development of infrastructure exchanges will most likely raise the volatility of the demand side. On the other hand, supply may shift due to new players urging into the cloud market. Generally, in case of a Shift in Demand or Supply, several actors are affected. *After Facebook bought Instagram lots of Instagram users switched to similar offerings and caused an overstressing of the respective infrastructure which in turn caused outages (Laurent 2013).*
	Bankruptcy / Buy-out	Going out of business through bankruptcy can cause permanent outage of cloud services (Armbrust et al. 2010; Troshani et al. 2011). Buy-outs may lead to a permanent or temporary outages, modified products, or a new pricing of the service. Bankruptcy and Buy-outs mostly affect small or medium sized cloud actors. *Large IT companies like Oracle and IBM bought a huge amount of small/mid-size Cloud companies during the last years.*

	Legal Issues	Being target of regulatory actions is an important non-technical issue for cloud actors (Armbrust et al. 2010). In case of legal actions against a vendor or another customer of the vendor, customers may suffer. Furthermore, government surveillance and intellectual property disputes (Jaeger et al. 2008) (and hence attorney-client privilege issues) rise as additional hazards in the context of Legal Issues. *Jansen (2011) describes that the FBI "raided computing centers in Texas and seized hundreds of servers, when investigating fraud allegations against a handful of companies that operated out of the centers".*
Reinforcer	Incompatibility	Today, cloud services often use proprietary protocols and interfaces (Dillon et al. 2010). Furthermore, initial service compatibility may fade over time, for example through updates, which makes diversification much more difficult. *Deviant update cycles can lead to incompatibility between former compatible actors. This incompatibility usually lasts only a few hours/days. Usually a vendor announces its forthcoming changes to the customers and the customer is able to react.*
	Lack of Transparency / Loss of Control	Migration to the cloud relinquishes control over the company's data and makes it dependent on the service vendor (Clarke 2010; Jansen 2011). Jansen (2011) state that actors that "subcontract some services to third-party service providers should raise concerns". Cloud services are often dependent on a single point of failure (Armbrust et al. 2010; Chow et al. 2009). *An outage can lead to a "cascade effect crippling all organisations dependent on that Cloud, and all those dependent upon them" (Marinos and Briscoe 2009). Due to the lack of transparency, an actor is not able to foresee such effects.*

	Unobtainability of Data / Lock-in	Large datasets at the vendor or proprietary interfaces often force customers to stay within its existing cloud environment (Armbrust et al. 2009). This lock-in of customers is profitable for the vendor (Armbrust et al. 2010) and increases the chance of opportunistic behavior on part of the vendor Clemons and Chen (2011). *Armbrust et al. (2009) compute that the transfer of 10 TB of data from U.C. Berkley to Amazon in Seattle would last over 45 days. A batch process with a huge amount of data is unable to perform with this speed. Additionally, the bandwidth is often quite volatile.*
	Automation Errors	Prater (2005) describes wrongly conditioned ERP systems in supply chain networks which cause "chaotic spikes" in the demand forecast of warehouse systems. Such problems, labelled Automation Errors, could also occur in cloud networks with automatized processes that may be wrongly conditioned and therefore lead to escalating risks. *Armbrust et al. (2009) describe that blacklisting of EC2 IP addresses by spam-prevention services may limit which applications can be effectively hosted.*
	Geographical Distribution of Network Actors	During the last years, data centers were built in areas with cheap energy, low temperature, and favorable legal position. Such preferred geological regions could pose a problem for cloud networks as for example natural disasters might hit different actors at the same time. *A lightning strike caused a power outage that led to an outage of datacenters of Amazon and Microsoft near Dublin (Miller 2011).*

Tab. III-2 Description of Description of Risks, Hazards, and Reinforcers

Hazard / Risk *If a hazard affects a risk, it is marked with "X".*	Data Security Issues	Data Privacy Issues	Price Risk	Loss of Data	Availability Issues
Technical Defects				X	X
User Errors	X	X		X	X
Security Issues	X	X		X	X
Natural Disasters			X	X	X
Legal Issues	X	X	X	X	X
Shifts in Demand and Supply			X		X
Bankruptcy / Buy-out			X	X	X

Tab. III-3 Relationships between hazards and risks

Reinforcer / Risk *If a reinforcer affects a risk, it is marked with "X".*	Data Security Issues	Data Privacy Issues	Price Risk	Loss of Data	Availability Issues
Incompatibilities				X	X
Lack of Transparency / Loss of Control			X		X
Unobtainability of Data / Lock-in			X	X	X
Automation Errors	X	X	X	X	X
Geographical Distribution of Network Actors				X	X

Tab. III-4 Relationships between reinforcers and risks

III.2 Beitrag 4: „Die Absicherung von Rohstoffrisiken – Eine Disziplinen übergreifende Herausforderung für Unternehmen“[1]

Autoren:	Gilbert Fridgen, Christian König, Philipp Mette Kernkompetenzzentrum Finanz- & Informationsmanagement, Lehrstuhl für BWL, Wirtschaftsinformatik, Informations- & Finanzmanagement (Prof. Dr. Hans Ulrich Buhl) Universität Augsburg, D-86135 Augsburg {gilbert.fridgen, christian.koenig, philipp.mette}@fim-rc.de Andreas Rathgeber Institut für Materials Resource Management, Professur für Wirtschaftsinformatik, insb. Finanz- und Informationsmanagement Universität Augsburg, D-86135 Augsburg andreas.rathgeber@mrm.uni-augsburg.de
Erschienen 2013 in:	ZfbF Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 65(2):167-190

Zusammenfassung:

Moderne Hightech-Produkte benötigen spezifische Rohstoffe verschiedener chemischer Elemente. Insbesondere die so genannten seltenen Erden spielen aktuell und künftig eine besonders wichtige Rolle. Dabei unterliegen Verfügbarkeit und Preis dieser Rohstoffe in hohem Maße einer durch viele Einflussfaktoren bedingten Unsicherheit. Da Unternehmen oftmals über Jahre hinweg an bestimmte Rohstoffe gebunden sind, müssen sie dieser Gefahr mit vielfältigen Strategien begegnen. Hierzu wird in diesem Beitrag ein Disziplinen übergreifender und praxisorientierter Gesamtüberblick über Rohstoffrisiken und mögliche Absicherungsmaßnahmen gegeben. Diese sollen zunächst vorgestellt und aus Unternehmenssicht strukturiert werden. Anschließend werden ausgewählte Absicherungsmaßnahmen zur Behandlung exemplarischer Rohstoffrisiken näher beleuchtet.

[1] Bei diesem Beitrag handelt es sich um eine redaktionell verbesserte Version des veröffentlichten Beitrags.

III.2.1 Einleitung

Die Entwicklung und Herstellung von modernen Produkten wie Mobiltelefonen, Flachbildschirmen, Windkrafträdern oder Photovoltaikanlagen benötigt eine stetig zunehmende Menge an Rohstoffen einer zunehmenden Anzahl verschiedener chemischer Elemente. Insbesondere die für Deutschland so wichtigen Zukunftstechnologien (Bleischwitz et al. 2009, S. VI) weisen eine hohe, stetig steigende Abhängigkeit von spezifischen Rohstoffen auf (Johnson et al. 2007, S. 1759). So werden beispielsweise für die Herstellung einer einzigen Windkraftanlage durchschnittlich zwei Tonnen des seltenen Metalls Neodym benötigt (Milmo 2010). Bei der Produktion von Flachbildschirmen und Mobiltelefonen sind zwar nur sehr geringe Mengen des Rohstoffs Indium nötig, verfügbare Alternativen ohne den Einsatz von Indium „sind aber den gängigen Lösungen hinsichtlich Produkteigenschaften und Produktionseffizienz unterlegen“ (Christen 2005, S. 61). Das zunehmende Interesse an diesen Produkten insbesondere auch aus den Schwellenländern, deren steigende Kaufkraft und die weiter wachsende Weltbevölkerung lassen eine noch weiter ansteigende Rohstoffnachfrage in der Zukunft erwarten, die „schon bald alle Grenzen sprengen“ (Radermacher/Beyers 2009, S. 12) würde. Obwohl fast alle Rohstoffe aus geologischer Sicht auf absehbare Zeit nicht von Knappheit bedroht sind, ist die Verfügbarkeit wirtschaftlich und politisch nutzbarer Lagerstätten zukünftig nicht gewährleistet. Hinzu kommt, dass die Erschließung einer neuen Mine bis zum regulären Förderbetrieb bis zu zehn Jahre dauern kann (o.V. 2009, S. W1). Verschärft wird diese Situation noch durch erdgeschichtliche Fakten: So wurden Rohstoffe bei der Erdentstehung aufgrund unterschiedlicher geophysikalischer Eigenschaften wie Schmelzpunkt oder Dichte ungleichmäßig verteilt und weisen länderspezifisch konzentrierte Vorkommen auf. Unter anderem als eine Folge davon kann die Volksrepublik China circa 97% der weltweiten Produktion von in der Erdkruste sehr selten vorkommenden Rohstoffen, den so genannten Metallen der seltenen Erden, fördern (European Commission 2010, S. 38). Aufgrund gestiegenen Eigenbedarfs werden dort jedoch die Exporte stetig gedrosselt, beispielsweise Mitte 2011 um 30% (o.V. 2011b, S. 65; Bradsher 2010, S. B4). Somit unterliegen Rohstoffe im Allgemeinen aufgrund der Unmöglichkeit der kurzfristigen Ausweitung des Angebots und der relativ preisunelastischen Nachfrage hohen Preisvolatilitäten, die in den allermeisten Fällen höher als Wechselkurs- und Zinsschwankungen sind (Bartram 2005 S. 163). Unternehmen binden sich aufgrund zum Teil langer Produkt- (wie zum Beispiel in der Flugzeugindustrie) oder Bauteillaufzeiten (wie zum Beispiel im Automobilbau oder in der Elektronikindustrie) teilweise über zehn Jahre an einen Rohstoff. Der strategische Einkauf von Rohstoffen erstreckt

sich in den meisten Unternehmen hingegen kaum auf einen längeren Zeitraum als zwei Jahre. Durch dieses Auseinanderklaffen können bei Unternehmen erhebliche Risiken schlagend werden. Dies kann tiefgreifenden Einfluss auf das Betriebsergebnis haben und in extremen Fällen sogar bis zur Zahlungsunfähigkeit führen (o.V. 2007, S. 2).

Dieser Gefahr können Unternehmen mit vielfältigen Absicherungsmaßnahmen begegnen. So beschäftigt sich die betriebswirtschaftliche Fachliteratur beispielsweise mit Rohstoffderivaten zur Risikoabsicherung (Buhl/Strauß/Wiesent 2011; Johnson 1960, S. 139-151; Chen/Lee/Shrestha 2003, S. 433-465) oder losgelöst davon mit der deterministischen Optimierung der Lagerbestände und Einkaufsketten, wobei bei letzterem die Risikoabsicherung bisher meist im Hintergrund steht. Materialwissenschaftliche und technische Aspekte bleiben dabei weitgehend unberücksichtigt. Natur- und ingenieurwissenschaftliche Disziplinen beschäftigen sich dagegen mit der Erforschung neuer Materialien, neuer technischer Möglichkeiten wie etwa der Miniaturisierung und Möglichkeiten zur Rohstoffsubstitution (Lee et al. 2009, S. 481-504; Fam/Rizkalla 2001, S. 280-289). Allerdings hat dort eine ökonomische Bewertung meist nur untergeordneten Stellenwert und berücksichtigt keine Aspekte der Risikoabsicherung, die durch eine Substitutionsoption ohne Zweifel vorhanden sein können. Folglich werden diverse Teilaspekte des vorliegenden Problems zwar tiefgehend beleuchtet, ein Disziplinen übergreifender und praxisorientierter Gesamtüberblick über Rohstoffrisiken, die auf Unternehmen einwirken und mögliche Absicherungsinstrumente gegen diese existiert jedoch nicht.

Aus diesem Grund werden im vorliegenden Beitrag zunächst typische Rohstoffrisiken gesammelt, vorgestellt und aus Unternehmenssicht strukturiert. Weiterhin werden mögliche ökonomische und technische Absicherungsmaßnahmen gegen Rohstoffrisiken beschrieben und eingeordnet. Schließlich werden beispielhaft ausgewählte Handlungsstrategien im Umgang mit Rohstoffrisiken beleuchtet. Auf diese Weise soll eine Grundlage für unternehmerische Entscheidungen, wissenschaftliche Forschung und Kooperationen von Wissenschaft und Praxis geschaffen werden.

III.2.2 Einführung in das Rohstoffmanagement

Als Rohstoffe werden alle Güter natürlichen, pflanzlichen oder mineralischen Ursprungs bezeichnet, die entweder nicht oder nur in einem für den Transport und Handel notwendigen Ausmaß be- oder verarbeitet sind (U.S. Office of Public Affairs 1948, IV-A, Article 56). Rohstoffe werden in aller Regel in erneuerbare Rohstoffe (Agrarrohstoffe, Vieh oder Wasser)

und nicht-erneuerbare Rohstoffe eingeteilt. Als nicht erneuerbar gelten Gesteine, Salze, metallische Rohstoffe wie Eisen, Aluminium oder Kupfer und fossile Rohstoffe wie Kohle oder Erdöl. Insbesondere bei metallischen Rohstoffen ist die Reproduzierbarkeit nur extrem eingeschränkt möglich, da diese durch die Zahl der Protonen und damit auch durch das Atomgewicht als Element des Periodensystems festgelegt sind (Elemente des Periodensystems können dabei nur durch Kernspaltung oder Kernfusion verändert werden). Elemente und damit auch Metalle, die ein geringes Atomgewicht aufweisen, wie Eisen, Kupfer und Aluminium sind auf der Erde relativ häufig zu finden. In letzter Zeit wurden aufgrund ihrer spezifischen Eigenschaften aber Metalle immer wichtiger, die sich durch ein hohes Atomgewicht auszeichnen, wie etwa Indium, Gallium oder Germanium. Diese Metalle werden dabei auch als seltene Metalle bezeichnet, da sie in der Erdkruste in einer Konzentration von weniger als 0,01 Gewichtsprozenten vorkommen (Skinner 1979, S. 4214). Diese sind jedoch für moderne Technologien aufgrund ihrer spezifischen Eigenschaften äußerst wichtig. So wurden mehr als 80% der Mengen, die seit 1900 aus mineralischen Lagerstätten gewonnen wurden, erst in den vergangenen 30 Jahren abgebaut (Bleischwitz et al. 2009, S. 6). Eine Untergruppe von seltenen Metallen, die so genannten Metalle der seltenen Erden, sind aufgrund ihrer Anwendungsmöglichkeiten im besonderen Fokus der Industrie. Im Gegensatz zu anderen seltenen Metallen existieren für Metalle der seltenen Erden weltweit nur vergleichsweise wenige Lagerstätten, da diese nur in kleinen Mengen und weit verstreut oder als Bestandteil in anderen Mineralien vorkommen.

Natur- und ingenieurwissenschaftlich gesehen richtet sich der Einsatz der verschiedenen Rohstoffe nach deren vielfältigen technischen Eigenschaften wie beispielsweise Brennwert, elektrische Leitfähigkeit, Magnetisierbarkeit, Wärmeleitfähigkeit, Verformbarkeit, Schmelz- und Siedepunkte oder die Eignung für Legierungen. Im Fokus der Wirtschaftswissenschaften stehen bei gegebenen Einsatzmöglichkeiten der Rohstoffe die beiden ökonomischen Kerneigenschaften *Preis* und *Verfügbarkeit* eines Rohstoffs (siehe Abbildung Abb. III-7). Andere möglicherweise ökonomisch relevante Eigenschaften wie Umweltverträglichkeit oder Exportbeschränkungen von Rohstoffen lassen sich grundsätzlich auf diese beiden Kerneigenschaften zurückführen. So ist die politisch intendierte Verknappung der Fördermenge eines Rohstoffs für ein Unternehmen zumindest kurzfristig nicht von direkter Bedeutung. Erst die mit der Verknappung einhergehenden Auswirkungen wie gestiegene Einkaufspreise oder verfügbarkeitsbedingte Produktionsausfälle besitzen ökonomische Relevanz.

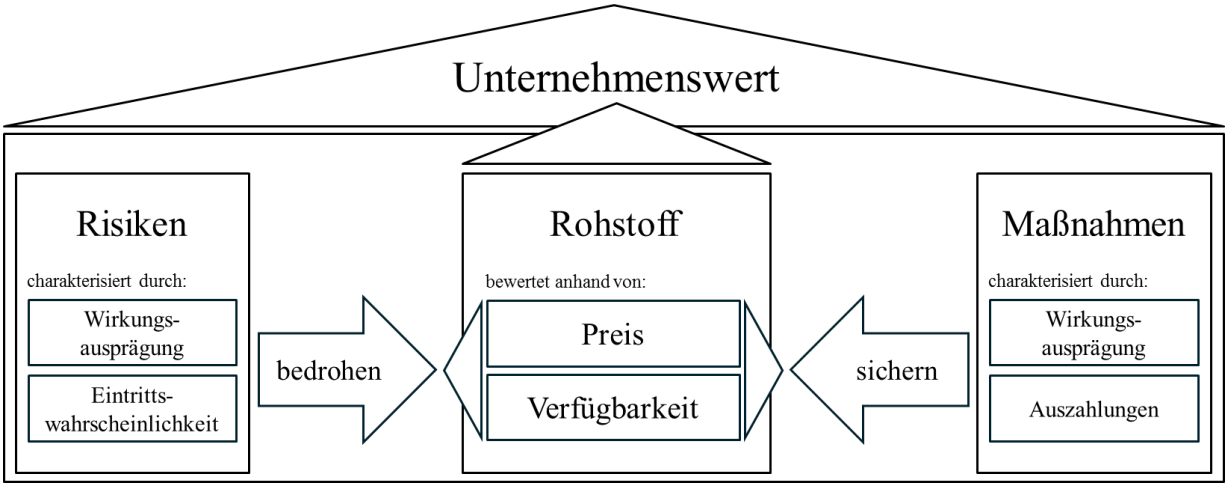

Abb. III-7 Die ökonomischen Kerneigenschaften von Rohstoffen zwischen Risiken und unternehmerischen Absicherungsmaßnahmen

Risiken, welche mit einer bestimmten *Wahrscheinlichkeit* eintreten, können Veränderungen der Ausprägungen der beiden ökonomischen Kerneigenschaften auslösen. Je nach ihrer *Wirkungsausprägung* können sie dabei auf den Preis, auf die Verfügbarkeit, oder aber auf beide Eigenschaften zugleich Einfluss nehmen. In diesen Fällen weichen realisierte Zahlungsströme, wie beispielsweise der Einkaufspreis eines Rohstoffs oder die Herstellkosten eines Produkts, von erwarteten Werten ab. Dies wird deutlich, wenn man den Unternehmenswert im Sinne der wertorientierten Unternehmensführung betrachtet. Dann lässt sich dieser als Barwert der zukünftigen risikobehafteten Zahlungsüberschüsse darstellen. Diese sind wiederum (neben vielen anderen Einflussfaktoren) von Rohstoffverfügbarkeit und Rohstoffpreisen abhängig:

$$Unternehmenswert =$$

$$= \sum_{t=0}^{\infty} \frac{EZ[Produktionsmenge(Rohstoffmenge, \dots)]_t - AZ[Rohstoffmenge\ und - preise, \dots]_t}{(1+i)^t}$$

(Kapitalkostensatz *i*, Planungszeitraum *t=0 bis* ∞, *Einzahlungen EZ* und *Auszahlungen AZ* als Funktion von Zufallsvariablen)

Steigende Rohstoffpreise erhöhen die Auszahlungen *AZ* und wirken wertsenkend. Mangelnde Verfügbarkeit senkt zwar die Einkaufsmengen und somit die Auszahlungen, wirkt aber andererseits auch einzahlungs- (*EZ*) und damit wertsenkend.

Gegen diese Risiken können sich Unternehmen durch die Nutzung von Absicherungsmaßnahmen schützen. Absicherungsmaßnahmen, welche zur Erreichung dieses Ziels eingesetzt werden können, lassen sich anhand der *Auszahlungen* ihres Einsatzes und anhand ihrer *Wirkungsausprägung* auf Preis- und/oder Verfügbarkeitsrisiken analog zu den Rohstoffrisiken kategorisieren. Dabei ist zu beachten, dass die Auszahlungsstruktur der Absicherungsmaßnahmen unterschiedlich ist (je nach Ausgestaltung einmalige Anfangsauszahlung oder periodisch wiederkehrende Auszahlungen für die Absicherung).

III.2.3 Rohstoffrisiken und Absicherungsstrategien im Unternehmensumfeld

III.2.3.1 Systematik

Die auf Unternehmen einwirkenden Rohstoffrisiken sowie mögliche Absicherungsmaßnahmen werden im Folgenden den verschiedenen Bereichen des Unternehmens und des Unternehmensumfelds zugeordnet. Dabei ist zu beachten, dass die Wirkung der Absicherungsinstrumente, die einem Bereich zugeordnet sind, im Regelfall nicht nur auf die in diesem Bereich auftretenden Rohstoffrisiken beschränkt ist, sondern oftmals auch die Absicherung von Risiken aus anderen Bereichen des Unternehmens und des Unternehmensumfelds ermöglichen. Die Menge aller verfügbaren Absicherungsinstrumente markiert den Möglichkeitsraum unternehmerischen Handels im Umgang mit den beschriebenen Herausforderungen. Von Bedeutung sind dabei auch die Schnittstellen zwischen Unternehmen und Unternehmensumfeld, welche sich auf die Anwendbarkeit eines Absicherungsinstruments auswirken können (beispielsweise die Verhandlungsmacht zu Kunden und Lieferanten). Abbildung Abb. III-8 stellt die Zuordnung von Rohstoffrisiken und Absicherungsmaßnahmen zu den Bereichen des Unternehmens und des Unternehmensumfelds im Sinne eines Ordnungsrahmens für das materialwissenschaftliche und ökonomische Rohstoffrisikomanagement dar.

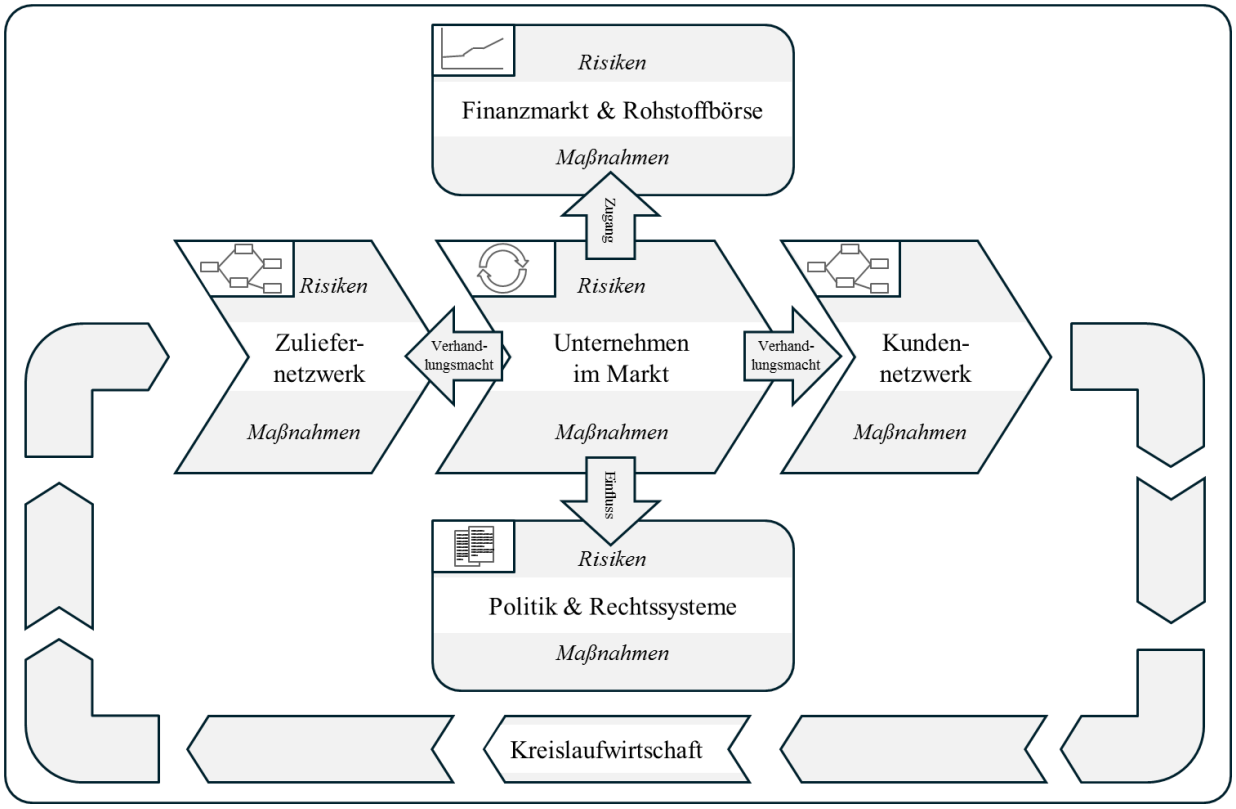

Abb. III-8 Bereiche des Unternehmens und des Unternehmensumfelds mit Rohstoffrisiken und Absicherungsmaßnahmen

Im Folgenden sollen die einzelnen Bereiche aus Abbildung Abb. III-8 kurz beschrieben werden, wobei einerseits die jeweiligen Rohstoffrisiken und andererseits mögliche Absicherungsmaßnahmen und deren Anwendung in der Praxis exemplarisch aufgeführt werden.

III.2.3.2 Unternehmen im Markt

Im Zentrum dieser Betrachtung stehen die Unternehmen, welche aus mehreren Abteilungen, wie Beschaffung, Produktion, Vertrieb oder Finanzen bestehen. Diese Abteilungen sind in unterschiedlichen Rollen am Produktionsprozess und somit an der Verarbeitung von Rohstoffen beteiligt. Diese Aufgaben- und Verantwortungstrennung birgt jedoch Potenzial für Rohstoffrisiken. Sind Unternehmensabteilungen unzureichend miteinander vernetzt oder erfolgt der Wissensaustausch nur wenig professionalisiert, so bestehen Mängel bei der Verknüpfung eigentlich vorhandener aber verteilter Informationen über Abhängigkeiten von einzelnen Rohstoffen. Ebenso können sich Rohstoffrisiken auch aus Informationsüberlastung oder aus mangelnder Verfügbarkeit von benötigten Informationen ergeben (Informationsflut bzw. Informationsmangel) (Krcmar 2009, S. 52). Entscheidungsträger verfügen daher heute

häufig gar nicht über die informatorische Ausstattung, um fundierte Entscheidungen über den Einsatz von Absicherungsmaßnahmen treffen zu können (Rohstoffrisiko: *Informationswirtschaftliches Ungleichgewicht*).

Das Unternehmen im Markt hat jedoch die Möglichkeit sich selbst gegen Rohstoffrisiken abzusichern. So können Maßnahmen und Methoden des modernen Informationsmanagements zur Schaffung einer tragfähigen informatorischen Ausgangssituation und somit zur Herstellung eines informationswirtschaftlichen Gleichgewichts beitragen (Absicherungsmaßnahme: *Unternehmensinternes Informationsmanagement*). Auch technische Maßnahmen beinhalten das Potenzial die Abhängigkeit von Rohstoffen zu reduzieren. So können Produktmodifikationen den Anteil kritischer Rohstoffe am Produkt verändern (Absicherungsmaßnahme: *Forschung & Entwicklung & Substitution*). Weiterhin besteht fast immer die Möglichkeit benötigte Rohstoffe zumindest kurz- bis mittelfristig auch physisch vorzuhalten (Absicherungsmaßnahme: *Lagerung*). Insbesondere beim unternehmensinternen Informationsmanagement besteht in der Praxis noch deutliches Verbesserungspotenzial. Neben IT-gestützten Lösungen zur Informationsbereitstellung muss ebenso durch die Organisationsstruktur des Unternehmens die Möglichkeit geschaffen werden, benötigte Informationen an zentraler Stelle verfügbar zu machen. Bisher wird dies durch die Trennung der Aufgabenbereiche von beispielsweise Einkauf und Finanzabteilung noch erschwert (KPMG 2007, S. 12), wobei sich der Einkauf gemäß einer Studie von Roland Berger gegenüber der Finanzabteilung meist zurückgesetzt fühlt (Roland Berger 2011). Nach einer Studie der Commerzbank nutzt zumindest jedes siebte von 4000 befragten mittelständischen Unternehmen Lagerung zur Absicherung von Risiken (Commerzbank 2011, S. 44). Forschung & Entwicklung wird nach einer Studie des Verbands der bayerischen Wirtschaft von 20% von ca. 2000 befragten Unternehmen des verarbeitenden Gewerbes in Bayern als Absicherungsmaßnahme eingesetzt (vwb 2011).

III.2.3.3 Zuliefernetzwerk

Zur Rohstoffbeschaffung nutzen Unternehmen ein Netzwerk aus meist mehreren Zulieferern, welche ihrerseits wiederum über ein Zuliefernetzwerk verfügen und auch ihrerseits untereinander in Beziehung stehen können. Zuliefernetzwerke sind daher häufig so komplex, dass Unternehmen keine genaue Kenntnis mehr haben, welche Beziehungen zwischen den einzelnen Netzwerkteilnehmern bestehen. Über mehrere Stufen der Lieferkette hinweg kann damit eine ganze Branche nur von wenigen Zulieferern oder Lagerstätten abhängig sein.

Mögliche Rohstoffrisiken entstehen deshalb durch die Gefahr eines Ausfalls einzelner zentraler Netzwerkteilnehmer (Rohstoffrisiko: *Lieferantenausfall*) oder aber durch Verfügbarkeitsschwierigkeiten am Anfang des Liefernetzwerks (Rohstoffrisiko: *Geologische Risiken / Unsichere Verfügbarkeit*). Darüber hinaus unterliegen die meisten Rohstoffe auch einem langfristig ansteigenden Preistrend (Clark 2005, S. 135), welcher auf Inflation und grundsätzliche Endlichkeit der Rohstoffe zurückzuführen ist (Hotelling 1931, S. 137-175; Krautkraemer 1998, S. 2065-2107) (Rohstoffrisiko: *Langfristiger Preisanstieg durch Verknappung*). Darüber hinaus sind durch die zum Teil zwischen den Zulieferern vorherrschenden komplexen Abhängigkeitsstrukturen auch systemische Risiken zu berücksichtigen, die in einem singulären Bereich auftretende Risiken in einem Dominoeffekt zu schwerwiegenden Auswirkungen für alle im System beteiligten Akteure werden lassen können (Rohstoffrisiko: *Systemische Risiken*).

Zur Absicherung von Preis- und/oder Verfügbarkeitsrisiken im Zuliefernetzwerk kann die Rohstoffbeschaffung von mehreren Zulieferern (Absicherungsmaßnahme: *Diversifikation*), die Bindung der Zulieferer durch langfristige Verträge mit vereinbarten fixen oder variablen Preisen (Absicherungsmaßnahme: *Langfristige Lieferverträge*), oder sogar die Rückwärtsintegration (Absicherungsmaßnahme: *Investition in Zulieferer*) genutzt werden. Diese Maßnahmen können umso besser durchgesetzt werden, je mehr Verhandlungsmacht ein Unternehmen gegenüber seinen Zulieferern ausüben kann. Darüber hinaus besteht die Möglichkeit durch Einkaufsgemeinschaften die Auftragsmenge zu erhöhen, um somit die Verhandlungsposition gegenüber Zulieferern zu stärken (Absicherungsmaßnahme: *Beschaffungskooperation*). Etwa die Hälfte der Unternehmen ist entsprechend der Studie der Commerzbank aufgrund der Marktentwicklungen aktuell auf der Suche nach neuen Lieferanten, um sich so breiter zu diversifizieren. Ein Viertel der Unternehmen versucht zudem, den steigenden Preisen durch Bildung von Einkaufsgemeinschaften zu begegnen. Langfristige Lieferverträge sind das mit etwa 80% am häufigsten genannte Absicherungsinstrument. Dagegen halten nur einige wenige Unternehmen eine Investition in Zulieferer für eine sinnvolle Möglichkeit und handeln demgemäß (Commerzbank 2011, S. 44).

III.2.3.4 Kundennetzwerk

Die aus Rohstoffen erstellten Produkte werden anschließend an ein Kundennetzwerk weitergegeben. Da die verwendeten Rohstoffe zu diesem Zeitpunkt damit bereits beschafft wurden, sowie die entsprechenden Preise im Regelfall bezahlt beziehungsweise ausgehandelt

wurden, bestehen bei der Weitergabe der Produkte an das Kundennetzwerk keine direkten Preis- und/oder Verfügbarkeitsrisiken. Nichtsdestotrotz können entsprechend flexibel gestaltete Lieferverträge mit mehreren Abnehmern zur Absicherung der Einzahlungen beitragen, beispielsweise bei sich ändernden Einkaufspreisen oder bei Lieferschwierigkeiten aufgrund von Verfügbarkeitsengpässen (Absicherungsmaßnahme: *Langfristige Lieferverträge*). Wie im Zuliefernetzwerk, so ist auch im Kundennetzwerk die Verhandlungsmacht entscheidend für die Umsetzung der Absicherungsmaßnahmen. So können Unternehmen in einer ungünstigen Verhandlungsposition gestiegene Preise ihrer Lieferanten nicht an ihre Kunden weitergeben, eine starke Verhandlungsposition kann hingegen neben gestiegenen Preisen möglicherweise auch zwischenzeitliche Verfügbarkeitsengpässe abfedern.

Gerne würden etwa zwei Drittel der Unternehmen Rohstoffrisiken auf ihre Kunden umlegen („Natural Hedging“) (KPMG 2007, S. 14), können dies aber oftmals aufgrund der Marktmacht dieser nicht umsetzen, wie beispielsweise in der Automobilzuliefererindustrie zu beobachten ist (o.V. 2007, S. 4). Bestärkt wird diese Beobachtung durch eine Studie aus dem Jahr 2006 bei 60 Einkaufsmanagern der größten Industrieunternehmen Österreichs. Hiernach gilt die Weitergabe von Preisrisiken an die Kunden als probates Absicherungsinstrument (A.T. Kearney 2006).

III.2.3.5 Finanzmarkt & Rohstoffbörse

An Finanzmarkt und Rohstoffbörse können grundsätzlich vorhandene Mechanismen und Strukturen zum Handel von Rohstoffderivaten genutzt werden. Durch ein gesteigertes Spekulationsvolumen ist es denkbar, dass die Volatilität der Preise über das fundamental gerechtfertigte Maß hinaus ansteigt, was bei Finanzinstrumenten teilweise bestätigt wurde (Shiller 1981, S. 421-436) (Rohstoffrisiko: *Preisschwankung durch Spekulation*).

Geeignete Hedging-Instrumente wie Optionen oder Futures können jedoch zur Absicherung gegen unsichere Preisentwicklungen genutzt werden. Je nach Ausgestaltung des Finanzinstruments ist dabei nur ein Preis (Barausgleich), oder aber die reale, physische Lieferung des Rohstoffs gesichert. Entscheidend ist hierbei die Verteilung der Rechte zwischen Käufer (Long) und Verkäufer (Short) in den jeweiligen Kontrakten. Bestimmte Derivate lassen sich dabei auch auf andere Bereiche außerhalb von Finanzmarkt & Rohstoffbörse übertragen. So kann das Rohstoffrisiko *Lieferantenausfall* zum Teil mit Finanzinstrumenten wie Credit Default Swaps abgesichert werden (Absicherungsmaßnahme: *Financial Hedging*). Je besser dabei der Zugang der Unternehmen zu Finanzmarkt und Rohstoffbörse ist, das heißt je geringer

vorherrschende Informations- und Transaktionskosten sind, desto einfacher und günstiger lassen sich Absicherungsmaßnahmen gegen Rohstoffrisiken im Bereich von Finanzmarkt & Rohstoffbörse anwenden. In der Praxis sichern sich heutzutage nur 10% der Unternehmen durch den gezielten Einsatz von Finanzinstrumenten gegen Rohstoffpreisrisiken ab. Zins- oder Währungsrisiken werden dahingegen von immerhin 40% der Unternehmen mit Finanzinstrumenten abgesichert. Als Gründe für dieses Missverhältnis geben Unternehmen an, dass die Absicherungsprodukte zu teuer, zu komplex und zu riskant seien (Commerzbank 2011, S. 59). Werden Finanzinstrumente zur Absicherung eingesetzt, handelt es sich dabei zumeist um Over-the-Counter-Produkte, da mit standardisierten Finanzinstrumenten die jeweiligen individuellen Risiken nicht vollständig aufgefangen werden können. Zumeist nutzen Unternehmen zur Durchführung dieser Absicherungsgeschäfte Großbanken oder spezialisierte Institute (KPMG 2007, S. 22). Dass dieses Ergebnis stark durch die Unternehmensgröße geprägt ist, zeigt die Studie von A.T. Kearney. Danach nutzten bereits im Jahr im Jahr 2006 ein Drittel der großen Unternehmen Finanzinstrumente zur Preisabsicherung (A.T. Kearney 2006).

III.2.3.6 Politik & Rechtssysteme

Bei fast allen unternehmerischen Aktivitäten sind rechtliche und politische Rahmenbedingungen zu beachten. Deren Veränderungen können direkt auf Preis und/oder Verfügbarkeit von Rohstoffen wirken (Rohstoffrisiko: *Zölle / Importbeschränkungen*). Auch unstetige politische Verhältnisse und schwache Rechtssysteme sowie die damit einhergehende Instabilität der Rohstoffexploration und -förderung haben das Potenzial, den Preis und die Verfügbarkeit von Rohstoffen stark zu beeinflussen (Rohstoffrisiko: *Politische Instabilität*).

Dem gegenüber steht die politische Arbeit unternehmerischer Interessensgemeinschaften (Lobbyarbeit), die eigene rohstoffpolitische Ziele in die Politik tragen und auf diese Weise eine Umsetzung ihrer Interessen forcieren (Absicherungsmaßnahme: *Organisation in Interessensgemeinschaften*). Die in diesem Handlungsfeld skizzierte Möglichkeit zur Absicherung von Rohstoffrisiken ist selbstverständlich stark vom politischen Einfluss des Unternehmens beziehungsweise dessen Entscheidungsträgern abhängig und schwer objektiv steuer- oder messbar. Die Eignung von Interessensgemeinschaften zur Absicherung gegen Rohstoffrisiken ist zudem abhängig von politischen und rechtlichen Räumen, in denen die Unternehmen agieren. In der Praxis mittelständischer Unternehmen werden die politischen Unterstützungsmaßnahmen zu 75% als eher schlecht bewertet (vbw 2011). Hier wünschen sich Unternehmen noch weitergehendes handelspolitisches Engagement in den Erzeugerländern, um

die Rohstoffversorgung sicherzustellen (Commerzbank 2011, S. 17). In der vbw Studie werden hier als dringlichste Maßnahmen von Seiten der Politik die Liberalisierung der Märkte und gute diplomatische Beziehungen zu den Ländern der Rohstofflieferanten genannt (vbw 2011, S. 35).

III.2.3.7 Die Bedeutung der Kreislaufwirtschaft als Absicherungsmaßnahme

Die Kreislaufwirtschaft spielt im Rahmen des Rohstoffmanagements eine Sonderrolle, da sie eine Absicherungsmaßnahme darstellt, aber gleichzeitig keine Rohstoffrisiken bedingt. Durch die Nutzung von recyclingfähigen Rohstoffen und wiederverwendbaren Bauteilen in einem „Closed-Loop"-System durch den Einsatz von technischen Maßnahmen kann die Abhängigkeit von Rohstoffen fast vollständig eliminiert werden (Bleischwitz 2010, S. 227-244) (Absicherungsmaßnahme: *Recycling, Reuse, Remanufacturing*). Dem entgegen steht jedoch eine schwierige und mitunter langfristige Einführung. So müssen die Unternehmen sicherstellen, dass die Kunden ihre Produkte/Rohstoffe nach der Nutzung oder nach dem Weiterverkauf wieder in das geschlossene System einspeisen. Darüber hinaus müssen die wiederaufbereiteten Produkte/Rohstoffe wieder den eigenen Zulieferern zugeführt werden, was nur in einer unternehmensübergreifenden Koordinationsleistung gewährleistet werden kann. Während 60% der befragten Unternehmen die Steigerung der Ressourceneffizienz als einen möglichen Weg zur Absicherung erkannt haben, nutzen nur etwa 30% Recycling als effizienzsteigernde Maßnahme (Commerzbank 2011, S. 20). Dass der Einsatz von Recycling als Absicherungsstrategie speziell für seltenere Elemente eine hervorragende Stellung einnimmt zeigte eine Befragung von 117 Experten aus Industrie und Technik (Achzet 2012).

III.2.3.8 Zusammenschau

Die in das vorgestellte Unternehmensumfeld eingeordneten Preis- und Verfügbarkeitsrisiken sowie mögliche Absicherungsmaßnahmen werden nun in einer integrierten Übersicht in Tabelle Tab. III-5 dargestellt. Auf diese Weise werden die Wechselwirkungen von Rohstoffrisiken und Absicherungsmaßnahmen deutlich, die wie beschrieben, typischerweise nicht auf einen einzelnen Unternehmensbereich beschränkt sind. Zusätzlich enthält die Tabelle Tab. III-5 eine grobe Einschätzung darüber, wie sich die aufgeführten exemplarischen Maßnahmen für die Absicherung gegen die jeweiligen Rohstoffrisiken eignen (+), bedingt eignen (o) oder nicht eignen (-). Im Rahmen dieser Betrachtung wird ersichtlich, dass Absicherungsmaßnahmen wie beispielsweise Forschung & Entwicklung & Substitution und Lagerung, die gegen sehr viele Rohstoffrisiken wirken, in der Praxis nicht in der zur erwartenden Häufigkeit eingesetzt werden (Forschung & Entwicklung bei 14% der befragten

Unternehmen, Lagerung bei 20%). Dementgegen eignen sich langfristige Lieferverträge nur in gewissen Fällen zur Risikoabsicherung, dennoch wird diese Absicherungsmaßnahme in der Praxis am häufigsten genutzt. Auf eine ausführliche Erklärung aller Einschätzungen muss an dieser Stelle aus Platzgründen verzichtet werden. Aufgrund des weiten Themenfeldes und der Zielsetzung dieses Beitrags kann und soll an dieser Stelle keine vollständige Aufarbeitung aller Rohstoffrisiken und Absicherungsmaßnahmen erfolgen. Vielmehr sollen nachfolgende Beispiele konkrete Fragestellungen für die Praxis aufzeigen und Denkanstöße zur Lösung individueller Probleme geben.

Exemplarische Zuordnung möglicher Maßnahmen zu möglichen Risiken		**Maßnahmen**																
		Unternehmen im Markt				**Zuliefernetzwerk**						**Kunden-netzwerk**		**Finanzmarkt & Rohstoffbörse**		**Politik & Rechtliche Rahmenbedingungen**		**Kreislauf-wirtschaft**
Risiken		Unternehmensinternes Informationsmanagement	Forschung & Entwicklung & Substitution	Lagerung	...	Diversifikation	Langfristige Lieferverträge	Investition in Zulieferer	Beschaffungskooperationen	Unternehmensübergreifend Informationsmanagement	...	Langfristige Lieferverträge	...	Financial Hedging	...	Organisation in Interessensgemeinschaften	...	Recycling, Reuse, Remanufacturing	...
Unternehmen im Markt	Informationswirtschaftliches Ungleichgewicht	+	-	-		-	-	o	+	+		-		-		o		-	
	...																		
Zuliefernetzwerk	Lieferantenausfall	-	+	+		+	-	o	o	o		o		o		-		o	
	Geologische Risiken / Unsichere Verfügbarkeit	-	+	+		o	-	-	-	-		o		o		-		o	
	Langfristiger Preisanstieg durch Verknappung	-	+	o		-	-	-	-	-		o		-		-		o	
	Systemische Risiken	+	+	+		o	o	o	o	+		o		o		-		o	
	...																		
Finanzmarkt & Rohstoffbörse	Preisschwankung durch Spekulation	-	+	+		-	+	o	-	-		o		+		-		o	
	...																		
Politik & Rechtliche Rahmenbedingungen	Zölle / Importbeschränkungen	-	+	+		+	-	-	-	-		-		-		+		o	
	Politische Instabilität	-	+	+		+	-	-	o	o		o		o		o		o	
	...																		

Legende:

+ Maßnahme kann im Allgemeinen zur Absicherung des Risikos eingesetzt werden.
o Maßnahme kann in gewissen Fällen zur Absicherung des Risikos eingesetzt werden.
- Maßnahme kann im Allgemeinen nicht zur Absicherung des Risikos eingesetzt werden.

Tab. III-5 Exemplarische Zuordnung von Absicherungsmaßnahmen zu Rohstoffrisiken

III.2.4 Ausgewählte Fragestellungen in Bezug auf unternehmerische Absicherungsmaßnahmen zur Sicherung von Rohstoffpreis und -verfügbarkeit

III.2.4.1 Die Nutzung von Kritikalitätsindizes als Frühwarnsystem für Rohstoffrisiken

Zur Prognostizierung von Rohstoffrisiken mit dem Ziel der Gewährleistung von ökonomischer Planungssicherheit werden so genannte Kritikalitätsindizes entwickelt. Ziel dieser Kritikalitätsindizes ist die einfache und fortwährende Bereitstellung von aggregierten Informationen hinsichtlich der Knappheit von Rohstoffen. Auf Basis dieser Informationen lassen sich Rückschlüsse auf zukünftige Preis- und Verfügbarkeitsrisiken ziehen. Aufgrund des hohen Maßes an Komplexität aggregieren Kritikalitätsindizes mehrere Risikofaktoren zu meist einer Kennzahl, die die Knappheit eines Rohstoffes bemisst (Achzet et al. 2010). Rosenau-Turnow et al. (2009) bestimmen das Verfügbarkeitsrisiko von Rohstoffen beispielsweise anhand der Risikofaktoren Rohstoffproduktions- und Förderkosten, geostrategische Risiken, Marktmacht von Unternehmen sowie heutiger und zukünftiger Angebots- und Nachfragesituation. Bauer et al. (2010) nutzen für den gleichen Zweck die Risikofaktoren grundlegende Verfügbarkeit, politische, regulatorische und soziale Faktoren, Produzentendiversifizierung, Technologienachfrage sowie Co-Abhängigkeit auf anderen Märkten. Für jeden Risikofaktor werden durch Expertenbefragung Schätzwerte gebildet, die durch eine Aggregationsvorschrift zu einem Kritikalitätsindex aggregiert werden. Zu diesen Pionierarbeiten der Kritikalitätsmessung sind jedoch einige methodische und inhaltliche Anmerkungen zu machen.

So werden die genannten Risikofaktoren nach Bauer et al. mit starren Gewichten aggregiert, Rosenau-Turnow et al. nehmen hingegen sogar nur eine grafische Aggregation in einem Spinnennetzdiagramm vor. Die Europäische Kommission (2010, S. 23) nutzt einen nach eigener Aussage „pragmatischen“ Ansatz zur Aggregation von Risikofaktoren. Auch eine quantitative und insbesondere monetäre Bewertung von Rohstoffrisiken findet durch Kritikalitätsindizes nur mit Einschränkung statt. Die existierenden quantitativen Methoden basieren dabei stets auf vergangenheitsbasierenden Daten, wobei eine statistische Überprüfung der Güte der Prognosewirkung noch nicht vorgenommen wird. Auch geschieht die Berechnung eines Kritikalitätsindexes in den meisten Fällen nur in Form von rohstoffspezifischen Einzelstudien und ist damit nicht täglich aktuell. Dies kann beispielsweise nach weltpolitischen Großereignissen unzureichend sein. Zudem betrachten existierende Ansätze Rohstoffrisiken zumeist nicht aus Unternehmenssicht sondern wenn überhaupt dann nur bezogen auf ganze

Branchen oder auf nationaler und volkswirtschaftlicher Ebene, wodurch die praktische Anwendbarkeit deutlich erschwert wird.

Nimmt man diese Beobachtungen zusammen, so wird ersichtlich, dass erstens eine weitergehende Erforschung von Kritikalitätsindikatoren aufbauend auf den genannten Pionierarbeiten dringend geboten ist. Zweitens zeigt sich, dass die Früherkennung von Rohstoffrisiken eine große Herausforderung für Unternehmen darstellt und dass deren Kern die erfolgreiche Verknüpfung verschiedener Disziplinen wie Geologie, Ökonomie, Ingenieurswissenschaft und Informationsverarbeitung ist.

III.2.4.2 Absicherung mittels Finanzderivaten, langfristigen Lieferverträgen und Lagerhaltung – ein kurzer Vergleich

Wie eingangs beschrieben sind für Unternehmen beim Einsatz von Absicherungsmaßnahmen deren Wirkung gegen Preis- und/oder Verfügbarkeitsrisiken eines Rohstoffs, sowie die dabei entstehenden Auszahlungen maßgeblich. Wirkung und Transaktionskosten als Auszahlungen für Beschaffung bis zum Einsatz in der Produktion sind jedoch nicht unabhängig voneinander. Gemäß der Theory of Storage (Kaldor 1939, S. 1-27) bildet sich der nicht vorhandene Zusatznutzen der ständigen Verfügbarkeit sogar im meist niedrigeren Abschlusspreis für börsengehandelte Futures im Gegensatz zum Preis bei Einlagerung ab (Normal Backwardation), was damit automatisch zu Transaktionskostenunterschieden zwischen den beiden Handlungsalternativen führt. Zu den beiden Absicherungsmaßnahmen, *Lagerhaltung* und *Financial Hedging* mit börsengehandelten Derivaten, treten noch *langfristige Lieferverträge* (auch OTC-Termingeschäfte), die im Folgenden hinsichtlich der Aspekte Wirkung und Transaktionskosten analysiert werden.

Es ist zu beobachten, dass für die physische Lagerung eines Rohstoffs im Vergleich zu den anderen genannten Absicherungsmaßnahmen typischerweise die höchsten Transaktionskosten, beispielsweise für Kapitalbindung und Einlagerung, nötig sind. So erfordern manche Rohstoffe beispielsweise technisch aufwendige Lager, da sie bei bestimmten Temperaturen oder mit in der Luft vorkommenden Gasen reagieren oder da sie als Umweltgifte gelten. Durch die physische Lagerung kann jedoch eine gleichzeitige Absicherung von Preis und Verfügbarkeit gewährleistet werden. Das Vorhalten der benötigten Rohstoffe schließt (zumindest entsprechend der Kapazität des Lagers und ohne Betrachtung unvorhergesehener Ereignisse wie zum Beispiel Diebstahl) die meisten Verfügbarkeitsrisiken aus. Darüber hinaus besteht sogar die Möglichkeit aus diesem Bestand auf zusätzliche Nachfrage vor dem geplanten

Absicherungszeitpunkt zu reagieren, so dass auch zwischenzeitliche Verfügbarkeitsrisiken gemildert werden können (Geman 2005, S. 24). Der je nach Absicherungsmaßnahme bestehende Mehrwert der Verfügbarkeit eines Rohstoffs wird dabei auch als Verfügbarkeitsprämie oder „convenience yield“ bezeichnet. Bei der Anwendung dieser Absicherungsmaßnahme sind die Unternehmen in natürliche Weise nicht mehr dem Risiko steigender Preise ausgesetzt, da diese bereits in der Vergangenheit bezahlt wurden.

Die Transaktionskosten für langfristige Verträge über die Lieferung von Rohstoffen zu fixen Preisen sind typischerweise geringer. Lagerkosten und gebundene Kapitalkosten fallen hier im Allgemeinen nicht an. Andererseits ist der Vorteil der vorzeitigen Verfügbarkeit des Rohstoffs nicht mehr gegeben, weil die convencience yield für den Besitzer eines gehandelten Rohstoffs, nicht jedoch für den Besitzer eines Liefervertrags existiert. Kann darüber hinaus der Zulieferer im Rahmen eines Liefervertrags jedoch selbst nicht mehr an den Rohstoff gelangen oder fällt er beispielsweise aufgrund von Insolvenz aus, so ist die Verfügbarkeit für die Vertragspartner trotz abgeschlossenem Liefervertrag auch zum Absicherungszeitpunkt nicht mehr sichergestellt. Aus diesem Grund kann die günstigere Absicherung über langfristige Lieferverträge als weniger wirkungsvoll im Vergleich zur physischen Lagerhaltung bezeichnet werden.

Betrachtet man weiterhin die Transaktionskosten für die Absicherung von Rohstoffrisiken über börsengehandelte Finanzderivate, so lässt sich feststellen, dass diese im Vergleich zur Lagerung und zu Lieferverträgen aufgrund der Standardisierung am geringsten sind. Die Standardisierung kann allerdings auch von Nachteil sein, da eine passgenaue Absicherung des benötigten Rohstoffs zum gewünschten Liefertermin und -ort in aller Regel nicht möglich ist. Somit können Unternehmen sich durch solche Derivate gegen Preisrisiken nur für bestimmte Laufzeiten vollständig oder ansonsten nur teilweise absichern. Je nach Ausgestaltung verbleiben ferner die Verfügbarkeitsrisiken bei den Unternehmen selbst, insbesondere wenn der Vertragspartner keine physische Lieferung plant, leisten kann oder keine Lieferung vertraglich vorgesehen ist. Beispielsweise bieten die zur Absicherung von Ölpreisschwankungen eingesetzten WTI Crude Futures (eine US-Ölsorte) die Möglichkeit der physischen Lieferung, Brent Crude Futures (eine europäische Ölsorte) sehen als Settlement nur einen Barausgleich vor (Geman 2005, S. 203 ff.).

Insgesamt zeigt sich ein Zielkonflikt zwischen der Wirkung der Absicherungsmaßnahme und den Kosten der Absicherung. Somit kann eine Auswahl möglicher Absicherungsmaßnahmen entsprechend des eigenen Sicherheitsstrebens beziehungsweise der Risikoaversion erfolgen,

das heißt gemäß der Wirkung auf Preis und/oder Verfügbarkeitsrisiken und den dafür anfallenden Auszahlungen.

Einschränkend darf aber nicht unerwähnt bleiben, dass Absicherungsmaßnahmen in gewissen Konstellationen auch gegenteilige Wirkung haben können: Sichert sich auf einem oligopolistischen Markt nur die Minderheit der Unternehmen beispielsweise über die Einlagerung von Rohstoffen ab, wobei die Mehrheit der Unternehmen sich keiner Maßnahme bedient, kann sich ein Preisverfall des Rohstoffs sehr negativ auf die Ertragssituation der Minderheit auswirken (Buhl/Strauß/Wiesent 2011). Im Endergebnis hat diese Minderheit durch ihr Handeln ein zusätzliches Risiko erzeugt.

III.2.4.3 Absicherung durch Forschung & Entwicklung & Substitution von Rohstoffen

Bestehen bei der Herstellung eines Produkts bezüglich eines verwendeten Rohstoffs Preis- oder Verfügbarkeitsrisiken, so haben Unternehmen gegebenenfalls die Möglichkeit, die angestrebte Funktionalität oder den Rohstoff selbst zu substituieren. Dabei wird unterschieden zwischen der Substitution von funktionalen Komponenten des Produkts (Funktionssubstitution) und der Neuentwicklung auf der Basis möglichst unkritischer Inhaltsstoffe bezüglich Preis- oder Verfügbarkeit (Materialsubstitution). Bei letzterer Variante sind die technischen und ökonomischen Eigenschaften des Substituts entscheidend. So ist es beispielsweise möglich, Kupfer bei der Herstellung von Klimaanlagen durch Aluminium zu ersetzen (o.V. 2011a). Aluminium ist das häufigste Metall in der Erdkruste und deutlich billiger als Kupfer: Der Preis für Aluminium entspricht aktuell circa einem Viertel des Preises von Kupfer (o.V. 2011c). Dabei muss beachtet werden, dass der substituierende Rohstoff veränderte technische Eigenschaften (hier: eine schlechtere Leitfähigkeit) besitzt. Oftmals sind die Substitutionsmöglichkeiten allerdings begrenzt. So kann die gleich hohe Energiedichte von Lithium in Akkus bei gleichzeitig langer Lebensdauer zum jetzigen Zeitpunkt von keinem anderen Rohstoff erzielt werden (Bleischwitz et al. 2009, S. 15). Zusätzlich zu den technischen Restriktionen sind bei der Substitution von Rohstoffen in der Produktion auch ökonomische Faktoren zu beachten. So sind Rohstoffe, die als Substitute für seltene Metalle mit gleichen oder ähnlichen technischen Eigenschaften verwendet werden sollen, oftmals ebenfalls seltene Metalle (beispielsweise beim Ersatz von Gallium durch Germanium), und damit meistens ebenfalls mit Preis- und Verfügbarkeitsrisiken behaftet, zudem werden sie auch teilweise gemeinsam gefördert (Roskill Information Services 2007).

Den Möglichkeiten aus der Substitution und eventuell daraus entstehenden Handlungsflexibilitäten stehen in aller Regel hohe Investitionsauszahlungen gegenüber. Die Wirtschaftlichkeit von Substitutionsinvestitionen ist dann maßgeblich von der weiteren Entwicklung der Rohstoffpreise beziehungsweise der Verfügbarkeit der Rohstoffe abhängig. Beachtenswert ist hierbei, dass sich die preisbestimmende Gruppe der Hauptnachfrager auf wenige Unternehmen begrenzt, so dass eine Substitutionsentscheidung bereits eines Nachfragers preisbeeinflussend sein kann. Durch die entstehende Nachfrageverschiebung sinkt der Preis des substituierten Rohstoffs ab und der Preis des substituierenden Rohstoffs steigt an. Auf diese Weise kann die Wirkung der Absicherungsmaßnahme deutlich vermindert bzw. konterkariert werden.

III.2.4.4 Recycling von seltenen Metallen

Eine nachhaltige Absicherungsmaßnahme gegen Preis- und/oder Verfügbarkeitsrisiken besteht für Unternehmen in der Wiederaufbereitung von Rohstoffen. Dazu sind der Aufbau eines Logistiknetzwerks zur Rückführung von ausgedienten Produkten wie auch der speziell im Falle von seltenen Metallen kostenintensive Einsatz moderner metallurgischer Verfahren notwendig. In diesen lassen sich zusätzlich zu den wichtigen seltenen Metallen auch assoziierte Elemente wie beispielsweise Zinn zurückgewinnen.

Entscheidend für die erfolgreiche Nutzung dieser Absicherungsmaßnahme sind neben der technischen Machbarkeit auch ökonomische Gegebenheiten wie Investitionszahlungen in Anlagen und laufende Auszahlungen für deren Betrieb. Weiterhin können beim Recycling beträchtliche Umweltauswirkungen verursacht werden, welche die Luft- und Wasserqualität einer Region massiv beeinträchtigen können (Sepúlveda et al. 2010, S. 28-41). Bei Lithium, welches beispielsweise für Akkus verwendet wird, ist der aktuelle Preis noch zu gering, um rentables Recycling zu betreiben (Bleischwitz et al. 2009, S. 4). Bei Indium ist der Einsatz geringer Mengen zwar für die Produktion von Flachbildschirmen unverzichtbar, ein Recycling ist jedoch ebenfalls nicht rentabel. Der Aufwand zur Rückgewinnung dieser geringen Mengen aus elektronischen Endgeräten ist gegenwärtig zu hoch. Beim Recycling des seltenen Metalls Tantal stehen Unternehmen hingegen vor technischen Hindernissen, da Tantal in Recyclingprozessen als Reststoff in Schlacke übergeht und aus dieser nur mit unverhältnismäßig großem Aufwand zurückgewonnen werden kann (Bleischwitz et al. 2009, S. 4).

Insbesondere bei den so genannten Gewürzmetallen erweist sich die Rückgewinnung als äußerst aufwendig. Gewürzmetalle sind bestimmte Metalle, die in Analogie zu Gewürzen für die Herstellung von Produkten in nur geringer Menge benötigt werden aber zugleich unverzichtbar sind. Zu ihnen zählen viele Metalle der seltenen Erden, aber auch seltene Metalle wie Indium oder Tantal. Für gewisse Einsatzzwecke können auch häufiger vorkommende Metalle wie beispielsweise Aluminium in geringer Dosis als Gewürzmetall dienen. Die Schwierigkeit der Absicherungsmaßnahme im Umgang mit Gewürzmetallen ergibt sich daraus, dass eine Rückgewinnung aus Abfällen durch die feine Verteilung von Gewürzmetallen in vielen Fällen äußerst aufwändig bis unmöglich ist.

Aus ähnlichen Gründen ist die Wiederaufbereitung von eingesetzten seltenen Metallen oftmals (noch) nicht ökonomisch rentabel, in anderen Fällen ebenfalls technisch schwierig bis unmöglich. Nichtsdestotrotz gibt es aber auch Beispiele für die erfolgreiche Anwendung der Absicherung durch Recycling. So arbeitet der Leuchtmittelhersteller Osram an der Rückgewinnung von seltenen Metallen, da die Preise für die bei der Leuchtmittelherstellung benötigten seltenen Metalle wie Lanthan, Europium, Terbium und Yttrium, stark angestiegen sind (Maier 2011). Um die erneute Nutzung benötigter Rohstoffe zu vereinfachen, kann es unter Umständen auch sinnvoll sein, schon in der Produktentwicklung und beim Vertriebskonzept darauf zu achten, dass die Wiederverwendung kompletter Bauteile (Remanufacturing) ermöglicht wird. Aufwändiges Einschmelzen kann so vermieden werden.

III.2.4.5 Einkaufsgemeinschaften zur Stärkung der Marktmacht

Gerade Unternehmen der Automobilzulieferindustrie stehen bei der Absicherung von Rohstoffrisiken vor einer besonderen Situation. Beschaffungsseitig stehen sie vor der Herausforderung, zum Teil seltene Rohstoffe von Zulieferern mit großer Marktmacht, wie zum Beispiel von chinesischen Staatskonzernen zu beziehen. Absatzseitig fordern Automobilhersteller langfristig feste Preise. Sie begegnen der Zulieferindustrie ebenfalls mit hoher Marktmacht. Diese zweiseitige Drucksituation sucht die deutsche Automobilindustrie gegenwärtig zu lösen. So haben auch die Automobilhersteller die Zwangslage ihrer Zulieferer verstanden und daraus potenzielle Risiken für sich selbst erkannt. Aus diesem Grund sind Deutschlands Automobilhersteller und ihre Zulieferer gerade im Begriff sich zu einer Einkaufsgemeinschaft zusammen zu schließen, um auf diese Weise ihre Marktmacht zu bündeln und ihre Einkaufskonditionen durch die dadurch erhöhte Auftragsmenge zu verbessern

(Fischer/Hucko 2011). Neben Unternehmen wie Bosch und Continental sind auch andere stark von Rohstoffen abhängige Industrieunternehmen wie Siemens an den Gesprächen beteiligt.

III.2.5 Zusammenfassung und Ausblick

Im vorliegenden Beitrag wurden die wesentliche Abhängigkeit der Industrie von Rohstoffen sowie die Rohstoffproblematik unter ökonomischen Gesichtspunkten dargestellt. Weiterhin wurden Rohstoffrisiken und unternehmerische Absicherungsmaßnahmen diskutiert und im Sinne eines Ordnungsrahmens zum Rohstoffrisikomanagement strukturiert dargestellt. Im Anschluss daran wurden ausgewählte praxisnahe Beispiele aus dem untersuchten Problembereich näher vorgestellt. Dabei wurde deutlich, dass eine Vielzahl an Rohstoffrisiken auf Unternehmen einwirken kann und vielfältige Absicherungsmaßnahmen zur Eindämmung derselben eingesetzt werden können.

Erscheint die Absicherung eines einzelnen Risikos lediglich ein Auswahlproblem zwischen verschiedenen Maßnahmen zu sein, so erhöht sich die Komplexität jedoch sprungartig durch die Betrachtung von mehreren Rohstoffrisiken, wie sie in der Realität typischerweise auftreten. Die Erarbeitung von Methoden zur ertrags- und risikoorientierten Zuordnung einer Vielzahl von Absicherungsmaßnahmen zu einer Vielzahl von Rohstoffrisiken im Rahmen eines effizienten Rohstoffrisikomanagements stellt eine große Herausforderung für Wissenschaft und Praxis dar. Wie gezeigt wurde ist beim Einsatz der Absicherungsinstrumente zudem auch zu beachten, dass dabei auch neue Risiken entstehen können.

Zur Bewältigung dieser Herausforderungen können sich Wissenschaft und Praxis nicht auf Lösungsansätze einzelner isolierter Disziplinen oder Unternehmensbereiche verlassen. Vielmehr muss in interdisziplinären Teams und in einer bereichsübergreifenden Anstrengung ganzheitlich gegen die ökonomischen Risiken der Rohstoffproblematik vorgegangen werden. Hier kann die unternehmensinterne und -übergreifende IT-Vernetzung als zentrales Nervensystem der Unternehmen einen wichtigen Beitrag leisten, um Risiken möglichst vollständig zu erfassen, ertrags- und risikointegriert zu bewerten und effektiv zu beseitigen. Nur so kann es möglich sein, ein aktives und vorausschauendes Rohstoffrisikomanagement mit einem effizienten Portfolio an Absicherungsmaßnahmen zu implementieren. Zur Bewältigung dieser Herausforderungen werden insbesondere Fachkräfte aus Wissenschaft und Praxis benötigt, die sowohl ökonomische als auch technische Eigenschaften sowie Wechselwirkungen zwischen eingesetzten Rohstoffen, Technologien, Risiken und Absicherungsmaßnahmen kennen und verstehen. Daraus ergibt sich die Anforderung, diese erforderlichen Kompetenzen

schon früh in der Ausbildung in sogenannten Schnittstellendisziplinen, wie beispielsweise Wirtschaftsingenieurwesen oder Wirtschaftsinformatik, zu vermitteln. Diesen Disziplinen fällt dabei als Gestalter und Vermittler eine zentrale Aufgabe zu.

III.2.6 Literatur

Achzet, Benjamin (2012), Empirische Analyse von preis- und verfügbarkeitsbeeinflussenden Indikatoren unter Berücksichtigung der Kritikalität von Rohstoffen, Dissertation, Lehrstuhl für Ressourcenstrategie, Universität Augsburg.

Achzet, Benjamin / Zepf, Volker / Meissner, Simon / Reller, Armin (2010), Strategien für einen verantwortlichen Umgang mit Metallen und deren Ressourcen, in: Chemie Ingenieur Technik, Vol. 82, S. 1913-1924.

A.T. Kearney (2006), Risikomanagement im Rohstoffeinkauf: Ungenützte Potenziale für Österreichs produzierende Industrie, Wien.

Bartram, Söhnke M. (2005), The impact of commodity price risk on firm value – An empirical analysis of corporate commodity price exposure, in: Multinational Finance Journal, Vol. 9, S. 161-187.

Bauer, Diana / Diamond, David / Li, Jennifer / Sandalow, David / Telleen, Paul / Wanner, Brent (2010), Critical Materials Strategy, U.S. Department of Energy.

Bleischwitz, Raimund / Hagelüken, Christian / Lang, Daniel / Meißner, Simon / Reller, Armin / Wäger, Patrick (2009), Seltene Metalle - Rohstoffe für Zukunftstechnologien, in: Schrift der Schweizerischen Akademie der Technischen Wissenschaften, Nr. 41, S. 1-32.

Bleischwitz, Raimund (2010), International economics of resource productivity – Relevance, measurement, empirical trends, innovation, resource policies, in: International Economics and Econ Economic Policy, Vol. 7, S. 227-244.

Bradsher, Keith (2010), China plans to reduce its exports of minerals, http://www.nytimes.com/2010/10/19/business/global/19mineral.html, Abruf am 24.11.2011.

Buhl, Hans Ulrich / Strauß, Sofie / Wiesent, Julia (2011), The impact of commodity price risk management on the profits of a company, in: Resources Policy, Vol. 36.

Chen, Sheng-Syan / Lee, Cheng-few / Shrestha, Keshab (2003), Futures hedge ratios: A review, in: The Quarterly Review of Economics and Finance, Vol. 3, S. 433-465.

Christen, Markus (2005), Die stofflichen Grenzen des Wachstums, in: Forschung und Technik, Vol. 286, S. 61.

Clark, Colin W. (2005), Mathematical Bioeconomics: The optimal management of renewable resources, John Wiley & Sons.

Commerzbank (2011), Rohstoffe und Energie: Risiken umkämpfter Ressourcen, Frankfurt am Main.

European Commission (2010), Critical raw materials for the EU: Report of the ad-hoc working group on defining critical raw materials, http://ec.europa.eu/enterprise/policies/raw-materials/files/docs/report-b_en.pdf. Abruf am 24.11.2011.

Fam, Amir / Rizkalla, Sami (2001), Behavior of axially loaded concrete-filled circular fiber-reinforced polymer tubes, in: ACI Structural Journal, Vol. 98, S. 280-289.

Fischer, Heimo / Hucko, Margret (2011), Autobauer schmieden Rohstoffpakt, in: Financial Times Deutschland, http://www.ftd.de/unternehmen/industrie/:seltene-erden-autobauer-schmieden-rohstoffpakt/60104323.html, Abruf am 24.11.2011.

Geman, Hélyette (2005), Commodities and commodity derivatives: Modelling and pricing for agriculturals, metals and energy, Wiley Finance.

Hotelling, Harold (1931), The Economics of Exhaustible Resources, in: The Journal of Political Economy, Vol. 39, S. 137-175.

Johnson, Jeremiah / Harper, Ermelinda / Lifset, Reid J. / Graedel, Thomas E. (2007), Dining at the periodic table: Metals concentrations as they relate to recycling, in: Environmental Science & Technology Vol. 41, S. 1759-1765.

Johnson, Leland L. (1960), The theory of hedging and speculation in commodity futures, in: The Review of Economic Studies, Vol. 3, S. 139-151.

Kaldor, Nicholas (1939), Speculation and economic stability, in: The Review of Economic Studies, Vol. 7, S. 1-27.

KPMG (2007), Energie- und Rohstoffpreise – Risiken und deren Absicherung, Frankfurt am Main.

Krautkraemer, Jeffrey A. (1998), Nonrenewable Resource Scarcity, in: Journal of Economic Literature, Vol. 36, S. 2065-2107.

Krcmar, Helmut (2009), Informationsmanagement, Springer.

Lee, Jung-Yoon / Yi, Chong-Ku / Jeong, Hoon-Sik / Kim, Sang-Woo / Kim, Jinkoo (2009), Compressive response of concrete confined with steel spirals and FRP composites, in: Journal of Composite Materials, Vol. 44, S. 481-504.

Maier, Angela (2011), Seltene Erden verteuern Energiesparlampen, in: Financial Times Deutschland, http://www.ftd.de/unternehmen/industrie/:preiserhoehung-seltene-erden-verteuern-energiesparlampen/60097903.html, Abruf am 24.11.2011.

Milmo, Cahal (2010), Concern as China clamps down on rare earth exports, in: The Independent, http://www.independent.co.uk/news/world/asia/concern-as-china-clamps-down-on-rare-earth-exports-1855387.html, Abruf am 24.11.2011.

o.V. (2007), Rohstoff-Risiken managen, https://www.globalbanking.db.com/docs/WiWo_Advertorial_Rohstoffe_0907.pdf, Abruf am 24.11.2011.

o.V. (2009), Hightech-Metalle werden knapp, in: DIE WELT 29.8.2009, S. W1.

o.V. (2011a), Aluminiumpreis wird von Kupfer mitgezogen, http://www.faz.net/artikel/S31721/rohstoffanlagen-aluminiumpreis-wird-von-kupfer-mitgezogen-30324096.html, Abruf am 24.11.2011.

o.V. (2011b), Große Tiefseelager entdeckt, in: €uro am Sonntag 9.7. - 15.7.2011, S. 65.

o.V. (2011c), Rohstoffdaten, http://www.finanzen.net/rohstoffe/, Abruf am 24.11.2011.

Radermacher, Franz Josef / Beyers, Bert (2009), Welt mit Zukunft – Überleben im 21. Jahrhundert, Murmann Verlag.

Roland Berger (2011), Purchasing-Excellence-Studie: Trends und Benchmarks im Einkauf 2011, München.

Rosenau-Tornow, Dirk / Buchholz, Peter / Riemann, Axel / Wagner, Markus (2009), Assessing the long-term supply risks for mineral raw materials – a combined evaluation of past and future trends, in: Resources Policy, Vol. 34, S. 161-175.

Roskill Information Services (2007), The economics of rare earths and yttrium, The Services Verlag.

Sepúlveda, Alejandra / Schluep, Mathias / Renaud, Fabrice G./ Streicher, Martin / Kühr, Rüdiger / Hagelüken, Christian / Gerecke, Andreas C. (2010), A review of the environmental fate and effects of hazardous substances released from electrical and

electronic equipments during recycling: Examples from China and India, in: Environmental Impact Assessment Review, Vol. 30, S. 28-41.

Shiller, Robert J. (1981), Do stock prices move too much to be justified by subsequent changes in dividends?, in: American Economic Review, Vol. 71, S. 421-436.

Skinner, Brian J. (1979), Earth Resources, Prentice Hall.

vbw Vereinigung der Bayerischen Wirtschaft (2011), Rohstoffsituation Bayern – keine Zukunft ohne Rohstoffe, München.

U.S. Office of Public Affairs (1948), Havana charter for an international trade organization, Washington, U.S. Government.

IV Ergebnisse und Ausblick

Dieses Kapitel beinhaltet neben einer Zusammenfassung der wesentlichen Erkenntnisse der Dissertationsschrift in Abschnitt IV.1 die Darstellung der Limitationen und mögliche Anknüpfungspunkte für weiteren Forschungsbedarf in Abschnitt IV.2.

IV.1 Ergebnisse

Das Ziel dieser Dissertationsschrift war es, einen Beitrag zur Risikoidentifikation und Risikosteuerung als Teilbereiche des Risikomanagements in IT-Sourcing-Netzwerken zu leisten. Hierzu wurden als Grundlage zunächst bilaterale IT-Sourcing-Beziehungen untersucht (Kapitel II). Dabei wurden Risikoidentifikation und Risikosteuerung im Kontext von Investitionsentscheidungen in Cloud-Computing-Services betrachtet und die jeweiligen Auswirkungen verschiedener Handlungsspielräume dargestellt. Des Weiteren wurden Marktrisiken in IT-Outsourcing-Projekten fokussiert und es wurde anhand eines mathematischen Modells untersucht, wie eine unter ökonomischen Gesichtspunkten optimale Absicherung dieser Risiken gestaltet werden kann und in welchen Fällen andere Ansätze zur Risikosteuerung vorteilhaft sind. Anschließend wurde der Fokus auf Netzwerkstrukturen erweitert, für die ebenfalls Ansätze zur Risikoidentifikation und Risikosteuerung betrachtet wurden (Kapitel III). Zunächst wurde ein IT-Sourcing-Netzwerk aus verschiedenen Cloud-Computing-Akteuren untersucht und auf Basis von Taxonomien und eines Referenzmodells ein Ansatz zur Risikoidentifikation darin vorgestellt. Des Weiteren wurde aufgrund des strukturverwandten Charakters die Identifikation und Absicherung von Rohstoffrisiken herangezogen und hierzu ein entsprechender Ordnungsrahmen entwickelt. Die zentralen Ergebnisse der Dissertationsschrift werden nachfolgend noch einmal separat für jeden Abschnitt zusammengefasst:

- Kapitel II verfolgte das Ziel, die Aspekte der Risikoidentifikation und Risikosteuerung zunächst in bilateralen IT-Sourcing-Beziehungen im Kontext von Cloud-Computing-Investitionsentscheidungen und IT-Outsourcing-Projekten zu untersuchen.

  Hierzu wurden in Beitrag 1 Cloud-Computing-Investitionen als neue Bereitstellungsform für IT-Leistungen im Rahmen des IT-Portfoliomanagements betrachtet. Die verschiedenen Handlungsspielräume, über die bei der Planung solcher Investitionen entschieden werden muss, wirken sich auf realisierbare Potenziale, aber auch Auszahlungsstruktur und Risiken aus. Um eine optimierte Gestaltung der Investitionen zu ermöglichen, ist zunächst die Kenntnis bezüglich möglicher Erträge,

Risiken und Abhängigkeiten notwendig. Daher wurde eine strukturierte Darstellung zur Identifikation von Cloud-Computing-spezifischen Einflussfaktoren auf Ertrag, Risiko und Komplexität bei Cloud-Computing-Investitionsentscheidungen entwickelt (Ziel II.1). Anhand der vorgestellten Dimensionen Flexibilität des Liefermodells, Flexibilität des Servicemodells und der zeitlichen Flexibilität lassen sich vorhandene Gestaltungsspielräume im Rahmen der Investitionsentscheidung einordnen (Ziel II.2). Darauf basierend und unter Einbezug der entwickelten strukturierten Darstellung der spezifischen Einflussfaktoren konnten die Auswirkungen auf realisierbare Potenziale und Risiken untersucht werden (Ziel II.2). Dabei bleibt festzuhalten, dass (i) der Wechsel von einer Public zu einer Private Cloud zu höheren Auszahlungen führt, zugleich jedoch viele Cloud-Computing-spezifischen Risiken auffängt, weshalb eine hybride Cloud hier als komplexe Mischlösung oftmals einen guten Kompromiss darstellt. Des Weiteren bleibt festzuhalten, dass (ii) die Homogenität von Services eine große Rolle spielt, wobei eine zunehmende Heterogenität mit steigenden Auszahlungen und höheren Risiken einhergeht. Zuletzt ist anzumerken, dass (iii) durch das Ausnutzen der zeitlichen Flexibilität eine positive Einflussnahme auf Ertrag, Risiko und Komplexität der Investition möglich ist, was jedoch ein aktives Gestalten der Cloud-Investition notwendig macht.

In Beitrag 2 wurde der Fokus auf Marktrisiken in IT-Outsourcing-Projekten gelegt, welche in der Forschung bisher nur qualitativ adressiert wurden. Diese Risiken können sich in Form eines Ausfalls des Anbieters aufgrund einer Insolvenz oder eines Vertrauensverlustes aufgrund eines Einbruchs des Aktienkurses manifestieren und in finanziellen Schäden für den Nutzer resultieren. In der Finanzkrise der letzten Jahre wurde die Bedeutung dieser Risiken zuletzt wieder unterstrichen, weshalb sie seitens der IT-Entscheider in Unternehmen keinesfalls vernachlässig werden dürfen. Daher wurde im Beitrag ein quantitativer Ansatz entwickelt, der auf Basis einer Hedging-Methode mittels von Finanzderivaten die Risikosteuerung von Marktrisiken erlaubt (Ziel II.3). Dabei werden gemäß der Risikoeinstellung des Entscheiders entsprechende Finanzinstrumente gekauft, die in bestimmten Fällen eine Auszahlung generieren, um den möglichen Schaden abzufangen. Des Weiteren wurde die Vorteilhaftigkeit der Methode in Abhängigkeit verschiedener Einflussfaktoren näher untersucht (Ziel II.4). Hier kann festgehalten werden, dass (i) solch ein Hedging-Ansatz zur Absicherung von Marktrisiken für Unternehmen grundsätzlich immer vorteilhaft ist, wenn ein adäquates

Finanzinstrument verfügbar ist. Zudem wurde erkannt, dass (ii) eine hohe Schadenswahrscheinlichkeit auf Seiten des Projektpartners aufgrund von hohen Hedging-Kosten zu einem geringen optimalen Hedging-Grad führt, wohingegen der günstige Einsatz von Hedging-Instrumenten und damit ein hoher Absicherungsgrad bei relativ sicheren Projektpartnern empfehlenswert ist. Zuletzt konnte festgestellt werden, dass (iii) eine steigende Passung des Hedging-Instruments auf die betrachtete Projektsituation den auf Basis dieser Methode empfohlenen Einsatzgrad ebenfalls erhöht.

- Ziel von Kapitel III war es, die Aspekte der Risikoidentifikation und Risikosteuerung auf Netzwerkstrukturen zu erweitern. Hierbei wurden IT-Sourcing-Netzwerke und Netzwerke zum Bezug von Rohstoffen betrachtet.

  In Beitrag 3 wurden aktuelle Entwicklungen im Bereich des Cloud Computing beschrieben, wie beispielsweise Standardisierung, Spezialisierung, steigende Abhängigkeiten zwischen verschiedenen Akteuren und neue Marktstrukturen. Diese Entwicklungen verwandeln die bisherige Cloud-Computing-Landschaft in komplexe IT-Sourcing-Netzwerke, in denen neue Risiken entstehen, die sich zwischen den vernetzten Akteuren ausbreiten können. Daher wurde in diesem Beitrag eine Darstellungsform für vernetzte IT-Sourcing-Beziehungen zwischen Cloud-Computing-Akteuren in Form eines Referenzmodells entwickelt, um innerhalb dieser Netzwerkstrukturen Transparenz zu schaffen (Ziel III.1). Darin abgebildet sind verschiedene Akteure, die anhand ihrer Position, ihres Geschäftsmodells und des jeweils gehandelten Produkts charakterisiert werden können. Eine genauere Untersuchung verschiedener Risiken und deren Klassifikation in auslösende Gefahren, resultierende Risiken und verstärkende Umstände liefert die Grundlage zur Darstellung der Risikoausbreitung innerhalb des Netzwerks (Ziel III.2). Das entwickelte Referenzmodell stellt damit eine Möglichkeit dar, (i) diese neuartigen Strukturen zu verstehen und übersichtlich zu visualisieren, sowie (ii) mögliche Risiken an unterschiedlichen Stellen des Netzwerks zu identifizieren und (iii) deren Ausbreitung und Konsequenzen für einzelne Akteure sowie das ganze Netzwerk zu erkennen. Somit kann das Verständnis für die komplexen Zusammenhänge innerhalb von IT-Sourcing-Netzwerken für Forschung und Praxis erhöht werden.

  Beitrag 4 thematisierte die Risikoidentifikation und Risikosteuerung von Rohstoffrisiken für Unternehmen, wobei erneut Netzwerkstrukturen zum Tragen

kommen. Hierzu wurde ein Disziplinen übergreifender Gesamtüberblick über Rohstoffrisiken und mögliche Absicherungsmaßnahmen erarbeitet. Zunächst wurde eine Einführung in das Rohstoffmanagement gegeben, bei der insbesondere die Bedeutung bestimmter Rohstoffe für Zukunftstechnologien herausgestellt wurde und die ökonomischen Kerneigenschaften von Rohstoffen für Unternehmen, Preis und Verfügbarkeit als Resultat des Wirkens von Risiken und Maßnahmen beschrieben wurden. Um eine strukturierte Identifikation von Rohstoffrisiken (Ziel III.3) zu ermöglichen, wurde ein Rahmenwerk entwickelt. Dieses stellt das Unternehmen in einem Netzwerk aus verschiedenen Akteuren und Einflüssen dar. Dabei wurden die Bereiche Unternehmen im Markt, Zuliefernetzwerk, Kundennetzwerk, Finanzmarkt & Rohstoffbörse, Politik & Rechtssysteme sowie Kreislaufwirtschaft herangezogen. Innerhalb dieser einzelnen Bereiche wurden Risiken identifiziert und beschrieben. Zur Risikosteuerung bestehen verschiedene Absicherungsmaßnahmen für das Unternehmen, die ebenfalls anhand des Rahmenwerks eingeordnet und beschrieben wurden (Ziel III.4). Ausgewählte Absicherungsmaßnahmen wurden detailliert vorgestellt und anhand ihrer Stärken und Schwächen charakterisiert. Zudem wurde eine Übersicht entwickelt, die eine exemplarische Zuordnung von Absicherungsmaßnahmen zu Risiken verdeutlicht. Es ist dabei anzumerken, dass Risiken in einem Bereich nicht zwangsweise mit Maßnahmen aus demselben Bereich begegnet werden muss. So eignet sich beispielsweise die Absicherungsmaßnahme Lagerung, um auf verschiedene Rohstoffrisiken wie Lieferantenausfall, unsichere Verfügbarkeit, systemische Risiken oder Preisschwankungen zu reagieren. Systemischen Risiken können jedoch auch mit anderen Absicherungsmaßnahmen adressiert werden, wie zum Beispiel mit einem unternehmensübergreifenden oder unternehmensinternen Informationsmanagement. Im Allgemeinen kann die unternehmensinterne und -übergreifende IT-Vernetzung als zentrales Nervensystem der Unternehmen einen wichtigen Beitrag leisten, um Risiken möglichst vollständig zu erfassen, ertrags- und risikointegriert zu bewerten und effektiv zu steuern.

IV.2 Ausblick

Aus den Limitationen der in dieser Dissertationsschrift enthaltenen Beiträge ergeben sich weiterführende Fragestellungen, welche zukünftigen Forschungsbedarf mit sich bringen.

Kapitel II adressiert Risikoidentifikation und Risikosteuerung in bilateralen IT-Sourcing-Beziehungen. In diesem Zusammenhang bestehen folgende Anknüpfungspunkte für künftige Forschung:

- In Beitrag 1 wurden verschiedene Einflussfaktoren auf Erträge, Risiken und Abhängigkeiten einer Cloud-Computing-Investition dargestellt. Hier bietet sich eine quantitative Untersuchung dieser Einflussfaktoren in der Praxis an, um künftige Ansätze zur Bewertung dieser Einflussfaktoren zu ermöglichen. Beispielsweise lassen sich mit dem Wissen bezüglich des Ausmaßes der Auszahlungen und der Schwere der damit einhergehenden Risiken künftig fundierter Entscheidungen bei der Wahl der verfügbaren Gestaltungsspielräume treffen.
- Des Weiteren sollte der in Beitrag 1 vorgestellte Entscheidungsprozess nach Kruschwitz (2007) für verschiedene weitere Cloud-Computing-Investitionsentscheidungen verprobt und somit weiter verfeinert werden. Dabei sollte ein besonderes Augenmerk auf die Verrechnung und Gewichtung verschiedener Einflussfaktoren gelegt werden, um jederzeit zu einer transparenten Entscheidung gelangen zu können.
- In Beitrag 2 wird ein mathematisches Modell zur Bestimmung des optimalen Hedging-Grades in IT-Outsourcing-Projekten entwickelt. Daraus folgen verschiedene technische Limitationen, die es künftig zu adressieren gilt: So wurde die Möglichkeit eines finanziellen Schadens auf einen ex-ante bekannten Zeitpunkt beschränkt. Um dies aufzulösen, könnten Verteilungen für die Wahrscheinlichkeit eines Schadenseintritts und dessen Höhe in Abhängigkeit der Zeit eingeführt werden. Daraus folgend würde die Forderung nach einem abgewandelten Hedging-Instrument resultieren, welches in der Lage wäre, zu jedem möglichen Schadenszeitpunkt auch eine Auszahlung zu leisten und nicht auf einen ex-ante zu definierenden Schadenszeitpunkt beschränkt wäre.
- Das vorgestellte Modell in Beitrag 2 adressiert Schäden, die entweder aufgrund einer Insolvenz oder eines Kurssturzes resultieren. Mittels der Einführung verschiedener Auslöser bei unterschiedlichen Zuständen des Aktienkurses des Projektpartners könnte

der Hedging-Ansatz erweitert werden, um auf zusätzliche Umweltzustände reagieren zu können.

- Des Weiteren bietet es sich insbesondere im Kontext von IT-Sourcing-Netzwerken an, das vorgestellte Modell aus Beitrag 2 für das gleichzeitige Hedging verschiedener Projektpartner zu verwenden. Konsequenterweise ist dabei dann das gesamte IT-Outsourcing-Projektportfolio in seiner Gänze zu bewerten (Lacity und Willcocks 2003). Zu berücksichtigen wären hierbei bestehende Ansätze des IT-Portfoliomanagements, wie beispielsweise von Verhoef (2005), Wehrmann et al. (2006), oder Zimmermann et al. (2008).

Kapitel III erweitert den Fokus hin zu Netzwerkstrukturen. Dabei bestehen folgende Anknüpfungspunkte für künftige Forschung.

- Da der in Beitrag 3 betrachtete Cloud-Computing-Markt ein äußerst dynamisches Umfeld ist, sind die bisher identifizierten Akteure und Risiken darin einem stetigen Wandel unterworfen. Daher ist eine regelmäßige Überprüfung dieser Akteure und Risiken notwendig, um das Referenzmodell an laufende Entwicklungen und sich verändernde Marktstrukturen anpassen zu können.
- In Beitrag 3 wurde bisher ein Realweltbeispiel mittels des entwickelten Referenzmodells instanziiert. Hier sind weitere beispielhafte Instanziierungen notwendig, um das Referenzmodell weiter zu verbessern und zusätzliche Erkenntnisse im Hinblick auf die Risikoausbreitung zu gewinnen. Bei einer entsprechend hohen Anzahl weiterer Realweltbeispiele wird die Verknüpfung der einzelnen Instanziierungen möglich, so dass eine Art „Cloud Network Map“ entwickelt werden könnte, um eine holistische Sichtweise auf die bestehenden Netzwerkstrukturen und die darin auftretenden Risiken zu ermöglichen.
- Das vorgestellte Referenzmodell in Beitrag 3 stellt eine Unterstützung für den Schritt der Risikoidentifikation in IT-Sourcing-Netzwerken dar. Damit ist die Grundlage für künftige darauf aufbauende Ansätze zur Bewertung dieser Risiken geschaffen. Dabei bietet sich eine Quantifizierung der Risiken auf Basis verschiedener Kriterien an. Beispielsweise könnte die Wahrscheinlichkeit der Ausbreitung in Verbindung mit dem Wert der Daten genutzt werden. Letzterer kann als monetärer Verlust bewertet werden (Gordon und Loeb 2002) und ist von der jeweiligen Art der Daten abhängig (Smith 2003). Des Weiteren bieten sich die Downtime-Kosten an (Patterson 2002) und

mögliche Strafzahlungen könnten ebenso in die Bewertung einbezogen werden (vergleiche Troshani et al. 2011, Dübendorfer et al. 2004)

- Auf Basis der in Beitrag 3 identifizierten Risiken und einer wie dargestellt möglichen Quantifizierung dieser Risiken sind künftig Ansätze zur Risikosteuerung zu entwickeln und zu untersuchen. Dabei kann möglicherweise auf bestehende Ansätze aus anderen Disziplinen zurückgegriffen werden, wie beispielsweise von Lieferantennetzwerken (vergleiche Ritchie und Brindley 2007, Norrman und Jansson 2004), oder auch auf Erfahrungen aus der Absicherung von Rohstoffrisiken (siehe auch Beitrag 4).
- Gemäß Beitrag 4 stellt die Absicherung eines einzelnen Rohstoffrisikos zunächst lediglich ein Auswahlproblem zwischen verschiedenen Maßnahmen dar. Da in der Realität jedoch mehrere verschiedene Rohstoffrisiken zugleich vorherrschen, sind geeignete Methoden notwendig, um auf Basis von ertrags- und risikoorientierten Überlegungen das optimale Maßnahmenbündel zu identifizieren. Dabei sind Wechselwirkungen zwischen einzelnen Risiken und Absicherungsmaßnahmen zu identifizieren und zu beachten, so dass dies idealerweise im Sinne eines „Risikoabsicherungsportfoliomanagements“ geschehen sollte.
- Wie unter IV.1 zu Beitrag 4 angemerkt, kann eine unternehmensinterne und -übergreifende IT-Vernetzung als zentrales Nervensystem der Unternehmen einen wichtigen Beitrag zur Identifikation, Bewertung und Steuerung von Rohstoffrisiken leisten. Hierzu gilt es, entsprechende konkrete Anforderungen an solche Informationssysteme zu erarbeiten und diese zunächst prototypisch zu verproben bevor diese anschließend in der Praxis eingeführt werden können.

Zusammenfassend wurden in dieser Dissertation verschiedene Fragestellungen der Risikoidentifikation und Risikosteuerung in IT-Sourcing-Netzwerken behandelt, wobei Erkenntnisse aus bilateralen IT-Sourcing-Beziehungen sowie weiteren Netzwerkstrukturen herangezogen wurden. Die Erkenntnisse dieser Dissertation stellen damit die Grundlage für einen künftigen holistischen Ansatz zum Risikomanagement in IT-Sourcing-Netzwerken dar, der auch Aspekte der Risikobewertung und des Monitorings beinhalten muss. Hierbei sollten zudem auch bestehende Ansätze des Cloud-Computing-Risikomanagements (vergleiche Zhang et al. 2010), des Risikomanagements in Netzwerken (vergleiche Hallikas et al. 2004) und der Network Governance (vergleiche Jones et al. 1997, Provian und Kenis 2007) einbezogen werden. Aufgrund des dynamischen Charakters von IT-Sourcing-Netzwerken und deren stetiger Weiterentwicklung sind auch in Zukunft Überprüfung, Verbesserung und Erweiterung

der hier vorgestellten Forschungsinhalte und -ergebnisse notwendig, um eine effektive Unterstützung des Risikomanagements leisten zu können. Es wäre wünschenswert, wenn künftige Forschung im Bereich des Risikomanagements in IT-Sourcing-Netzwerken von den Ideen und Erkenntnissen dieser Dissertationsschrift profitieren könnte.

IV.3 Literatur

Dübendorfer T, Wagner A, Plattner B (2004) An economic damage model for large-scale internet attacks. 13th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises

Gordon LA, Loeb MP (2002) The economics of information security investment. ACM Transactions on Information and System Security 5(4):438-457

Hallikas J, Karvonen I, Pulkkinen U, Virolainen V, Tuominen M (2004) Risk management processes in supplier networks. International Journal of Production Economics 90(1):47-58

Jones C, Hesterly W, Borgatti S (1997) A General Theory of Network Governance: Exchange Conditions and Social Mechanisms. The Academy of Management Review 22(4):911-945

Kruschwitz L (2007) Investitionsrechnung. Oldenbourg Wissenschaftsverlag, München

Lacity MC, Willcocks LP (2003) IT Sourcing Reflections: Lessons for Customers and Suppliers. WIRTSCHAFTSINFORMATIK 45(2):115-125

Norrman A, Jansson U (2004) Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. International Journal of Physical Distribution & Logistics Management 34(5):434-456

Patterson DA (2002) A Simple Way to Estimate the Cost of Downtime. Proceedings of LISA '02: Sixteenth Systems Administration Conference, Berkeley, USA

Provian K, Kenis P (2007) Modes of Network Governance: Structure, Management, and Effectiveness. Journal of Public Administration Research and Theory 18(2):229-252

Ritchie B, Brindley C (2007) Supply chain risk management and performance: A guiding framework for future development. International Journal of Operations & Production Management 27(3):303-322

Smith DM (2003) The cost of lost data. Journal of Contemporary Business Practice 6(3):1-9

Troshani I, Rampersad G, Wickramasinghe N (2011) On Cloud Nine? An Integrative Risk Management Framework for Cloud. Proceedings of 24th Bled eConference, Bled, Slovenia

Verhoef C (2005) Quantifying the value of IT-investments. Science of Computer Programming 56(3):315-342

Wehrmann A, Heinrich B, Seifert F (2006) Quantitatives IT-Portfoliomanagement: Risiken von IT-Investitionen wertorientiert steuern. Wirtschaftsinformatik 48(4):234-245

Zhang X, Wuwong N, Li H, Zhang X (2010) Information security risk management framework for the cloud computing environments. Proceedings of the 10th International Conference on Computer and Information Technology, Bradford, UK

Zimmermann S, Katzmarzik A, Kundisch D (2008) IT Sourcing Portfolio Management for IT Service Providers - A Risk/Cost Perspective. Proceedings of the 29th International Conference on Information Systems (ICIS), Paris, France